# Tools of the trade

- Commercial forensics tools:
  - Enterprise versions are very costly
  - Complicated
  - Steep learning curve
  - Require expensive full-time resources
  - Heavily forensics-focused, not recovery-focused
  - Mostly bulky, slow and painfully "thorough"
- Other enterprise "security tools" (e.g., Scanners, AV, HIPS):
  - Poorly configured, not watched
  - Not widely or consistently deployed
  - Require problematic integration with infrastructure
- Free/Open source tools:
  - Mixed capabilities
  - Enterprise design not in mind

# Bottom line

You need the 10-day solution,
not the 90-day solution

# Critical data is easy to get

- There is a limited set of **critical data** that an analyst must be able to quickly *search* and *retrieve* to identify a majority of common infections:
  - Disk indicators: file name, size, hash, PE characteristics
  - Memory indicators: process name, loaded modules, command line arguments, strings in heap
  - Registry indicators: GUIDs and other static values
- Codeword's main purpose is to quickly expose this information in a meaningful way, so that an analyst can come to a reasonable conclusion about an enterprise-wide, active infection in minutes to hours
- Of course, it also has more advanced features ;-)

# Codeword inspiration

- **Frustration** with commercial forensics tools
  - Bugs
  - Time wasted on service calls
  - Licensing headaches
  - Inconsistent results (v5.5a != v6.5.1 ??)
  - Over-engineered, misses the simple use cases
  - Core capabilities aren't customizable
  - Lacking robust rootkit detection
- Fruitless search for a comprehensive **open-source alternative**
- The **agile**, responsive attitude of Codeword fits perfectly with RETRI

# Codeword goals

- Imagine combining these enterprise tools into one simple, easy-to-use tool:
  - Vulnerability & AV scanners – Codeword uses signatures to detect and scan host locally
  - Enterprise forensic tool – Codeword uses forensic techniques to collect malware evidence in an agent-based framework
  - Rootkit detection – think GMER or Ice Sword
- Extensible – define what you consider to be malicious
- Free…

# Current Capabilities

- **Detection -**Uses registry, file and memory "signatures" to detect malware and misconfigurations and heuristics to identify anomalous behavior
- **Evidence collection** – collects any malicious files discovered
- **Reporting** - Results are collected, compressed/encrypted and uploaded to a secure location in the Qnet (Sftp, http, smtp, or network share)
- **Mitigation** – disable devices, uninstall apps, change system policies, etc
- **Cleanup** – kill processes/threads, delete/rename files, delete/clear registry entries, restore boot sector
- **Remote Analysis**– connect to agent from admin interface

# Major Features

- Write your own **signatures** to find malware
  - **Simple** signature logic – use file names, sizes, hashes, etc
- Tweak advanced **heuristics** for better detection
  - **User** mode, **kernel** mode, and **low-level** heuristics
- **Isolate**, **clean** and **prevent** future reoccurrence of infections
- **Thorough** detection –Codeword searches the computer's registry, hard drives and removable media, and live system memory for evidence of infection
- Receive **usable** alerts and data – collect all relevant evidence, along with meaningful log files and summary reports, and ships those back to you over a reporting method of your choice.
- Real-time, remote analysis – connect to agents over encrypted tunnel

# Benefits and other uses

- Can be used on a regular basis as part of a network security best practice
- Use as a triage tool (e.g., in support of RETRI)
- Aggregate information on all system infections by site name and location
- Help find original infection point:  All malware and system information, including pinpointing USB devices, is reported back

# With that said…

- Codeword is not a "Forensically-sound" tool
- It will not solve all of your problems
- You should use Codeword as part of an overarching response process, not as The Easy Button


- Codeword is beta freeware – don't complain when it crashes
- Comes with no warranties or hypno-toads

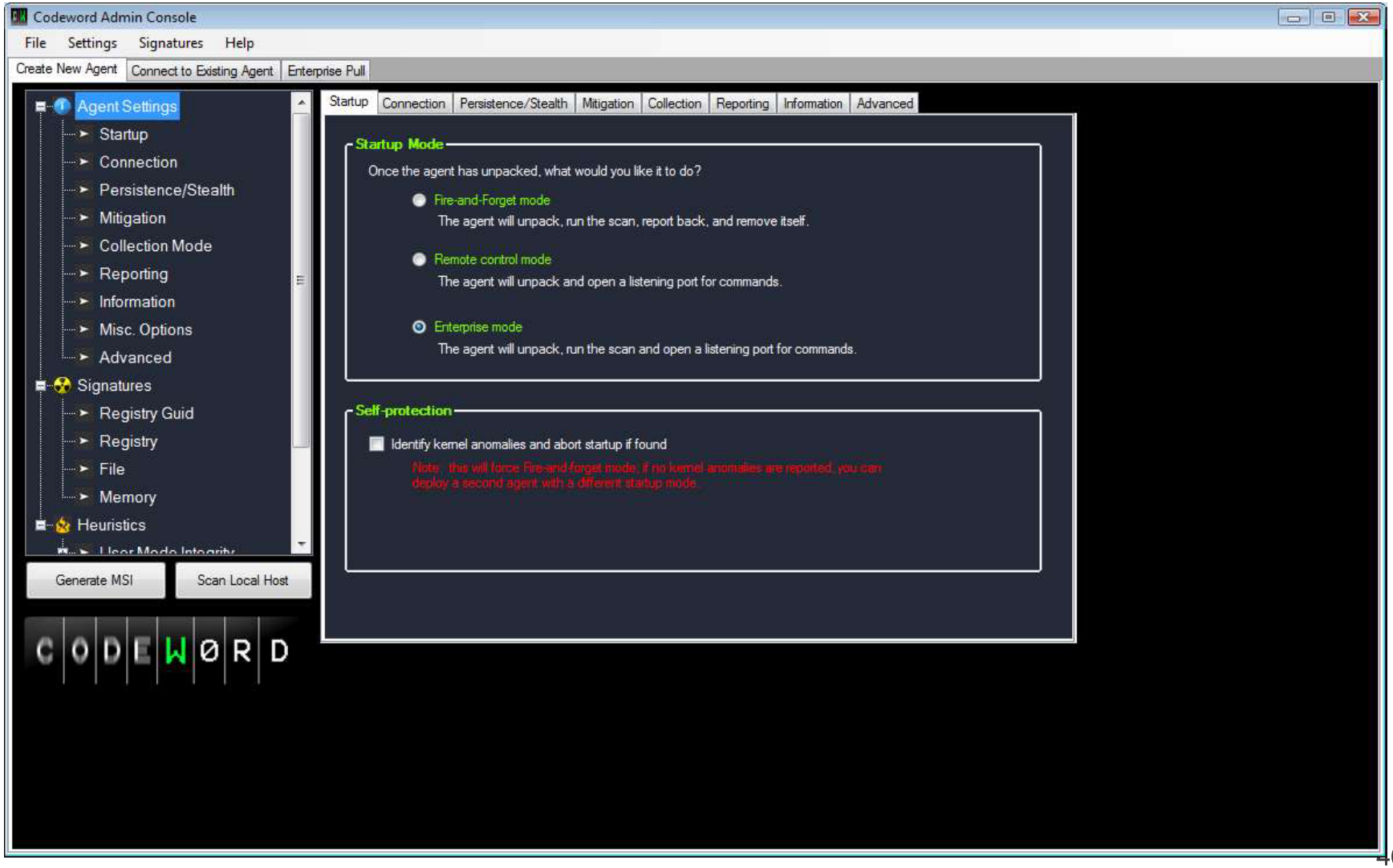
# Components

- Codeword has 3 primary components:
  - **Admin Console (C#)**: A graphical interface used to generate new agents and connect to existing deployed agents; wraps agent binary in an MSI installer file for deployment
  - **Agent (C#)**: A single binary contained inside the generated MSI; a host-level scanner to detect viruses, clean related files and footprints, and to implement remediation actions to prevent further infection
  - **Kernel-mode driver (C)**: A single SYS file that contains rootkit detection logic and other evidence-collecting code

# Quick start: using Codeword

1. Create an agent
   - Define signatures specific to malware
   - Choose user mode and kernel mode heuristics
   - Generate agent MSI installer
   - Deploy using psexec, sms, altiris, etc.
2. Connect/scan/analyze
   - Fire-and-forget mode: agent automatically sends an encrypted zip archive with results/evidence
   - Enterprise/Remote Control: use Admin Console
3. Collect/Mitigate

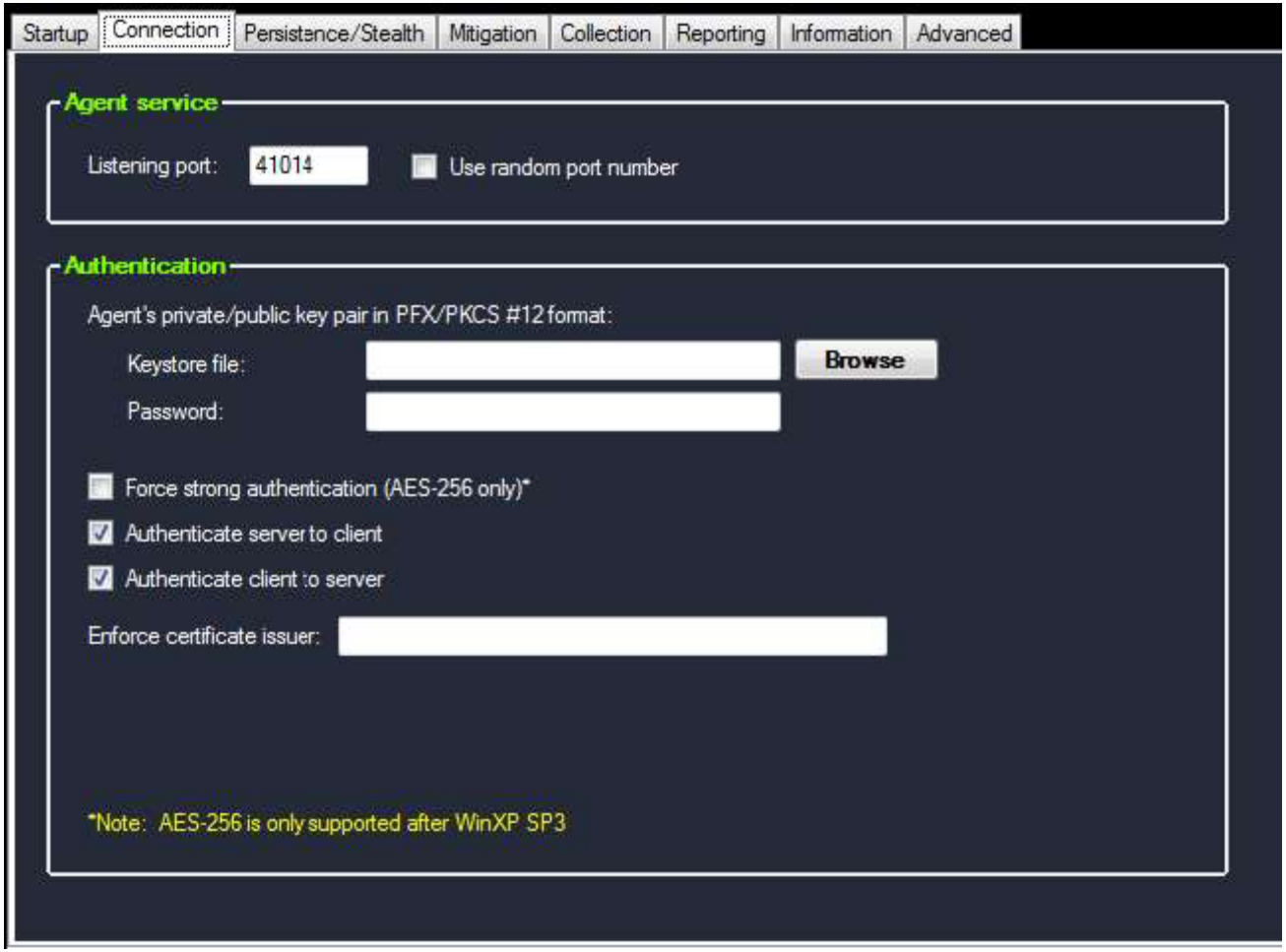
# Admin Console



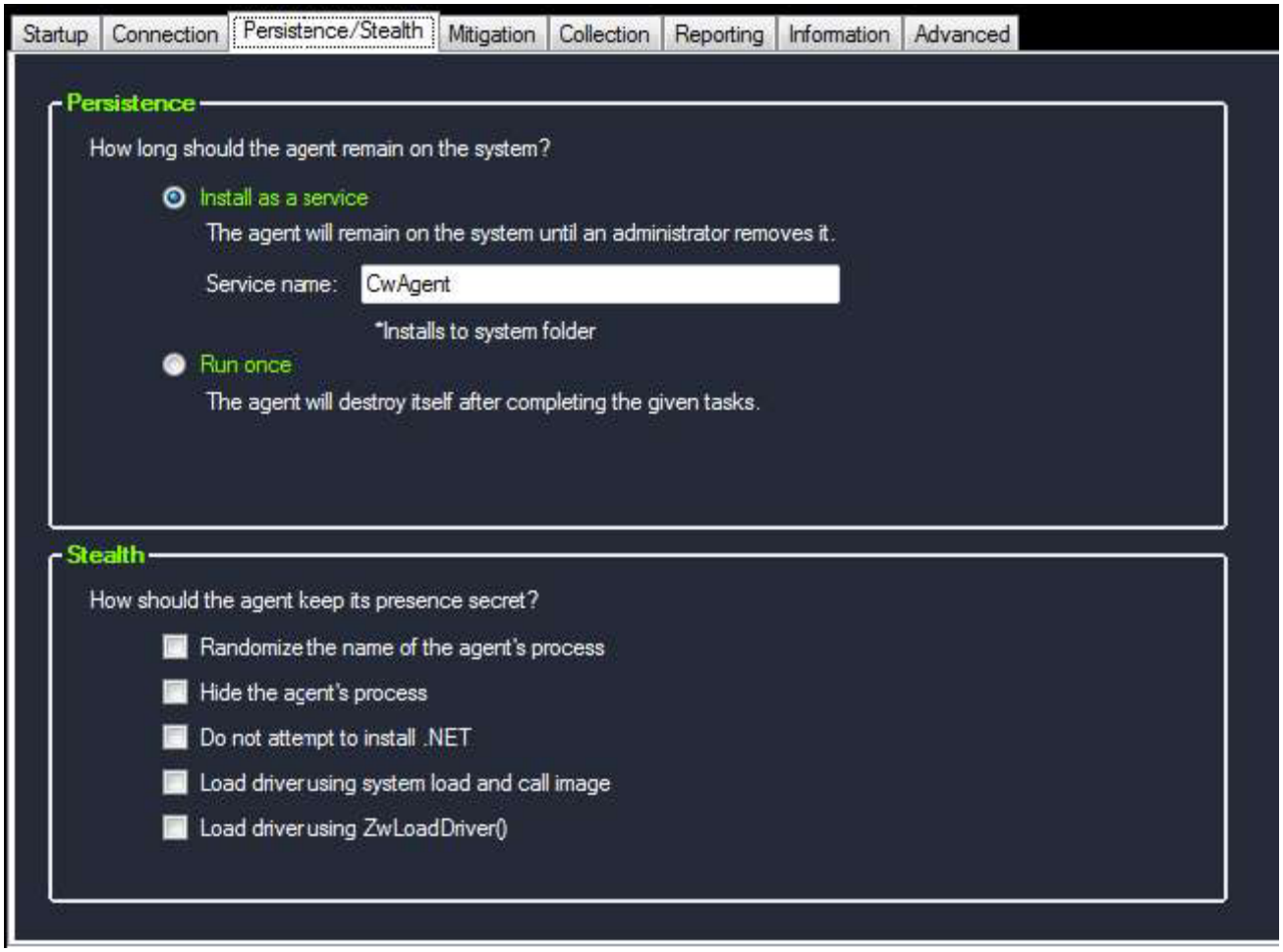
# Step 1: Create an agent

# Startup modes

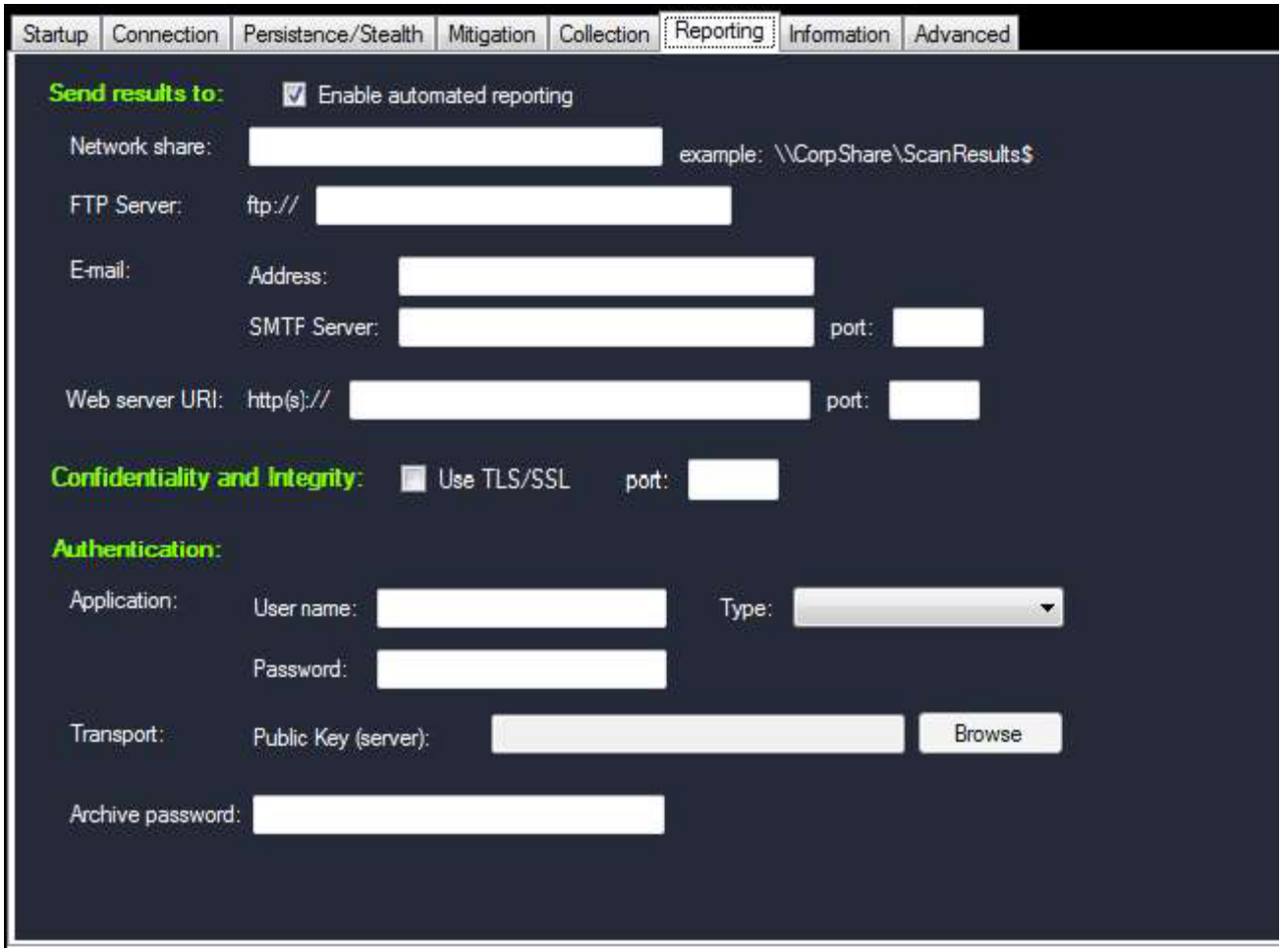
# Connection


Startup
Connection
Persistence/Stealth
Mitigation
Collection
Reporting
Information
Advanced
Agent service
Listening port:
41014
Use random port number
Authentication
Agent's private/public key pair in PFX/PKCS #12 format:
Keystore file:
Browse
Password:
Force strong authentication (AES-256 only)*
Authenticate server to client
Authenticate client to server
Enforce certificate issuer:
*Note: AES-256 is only supported after WinXP SP3

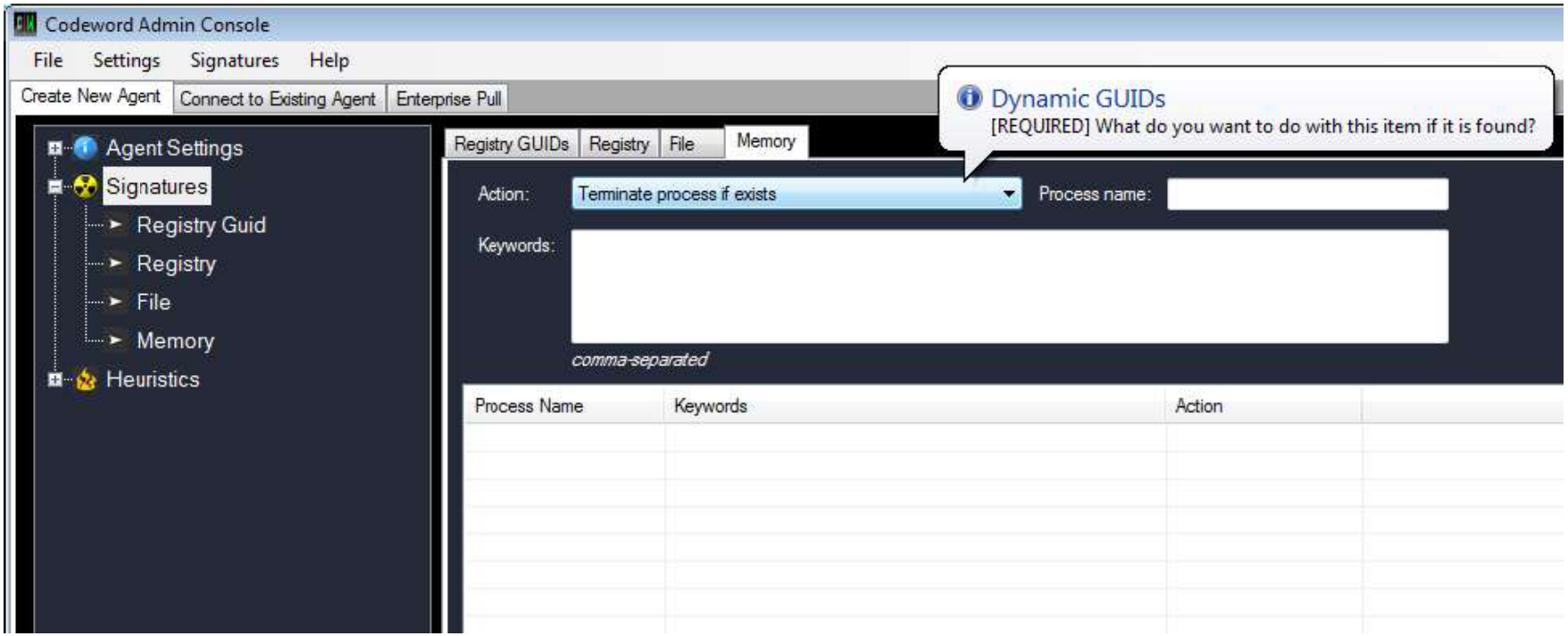
# Persistence/Stealth



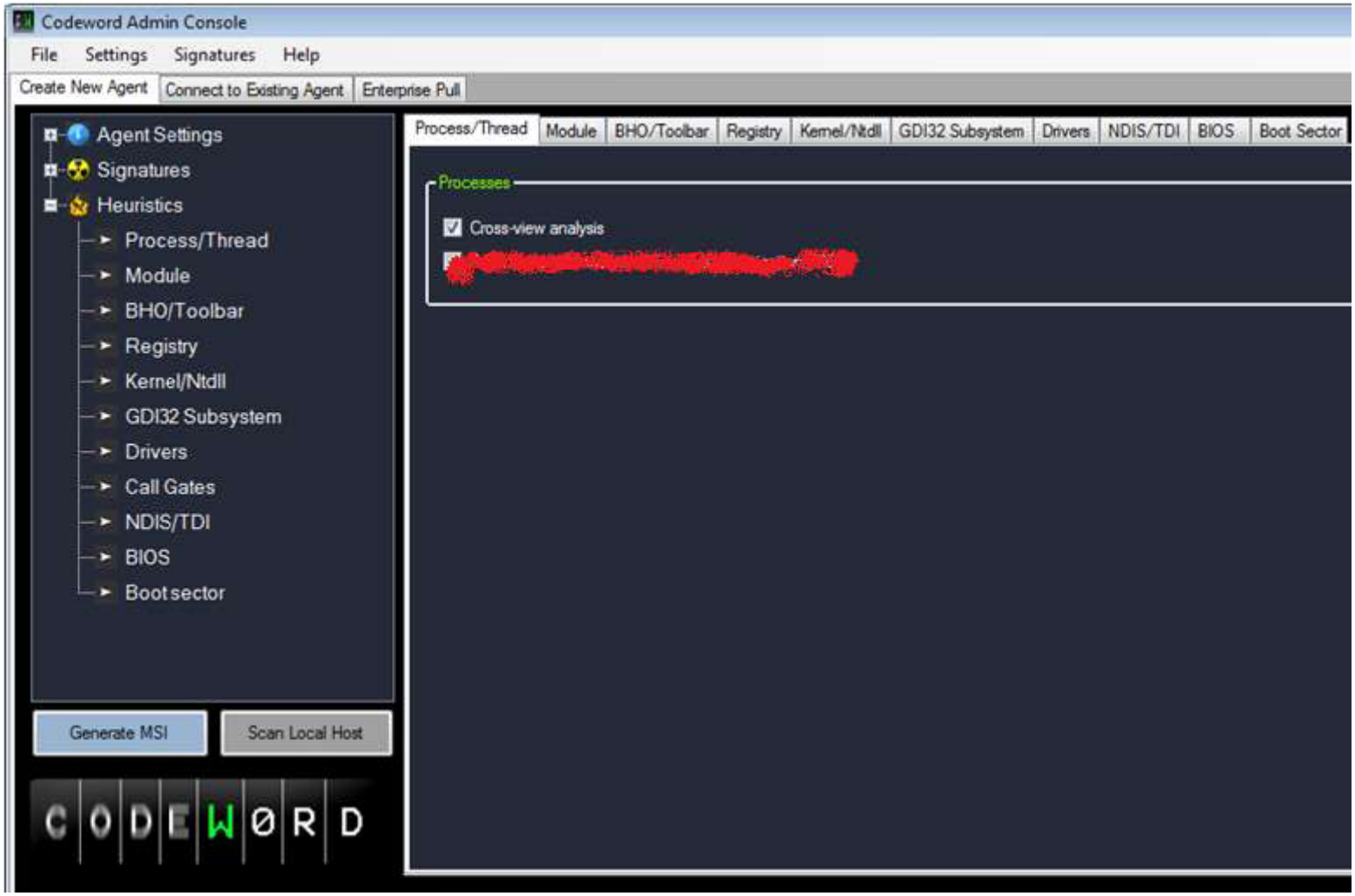
# Reporting


Startup
Connection
Persistence/Stealth
Mitigation
Collection
Reporting
Information
Advanced
Send results to:
Enable automated reporting
Network share:
example: \\CorpShare\ScanResults$
FTP Server:
ftp://
E-mail:
Address:
SMTP Server:
port:
Web server URI:
http(s)://
port:
Confidentiality and Integrity:
Use TLS/SSL
port:
Authentication:
Application:
User name:
Type:
Password:
Transport:
Public Key (server):
Browse
Archive password:

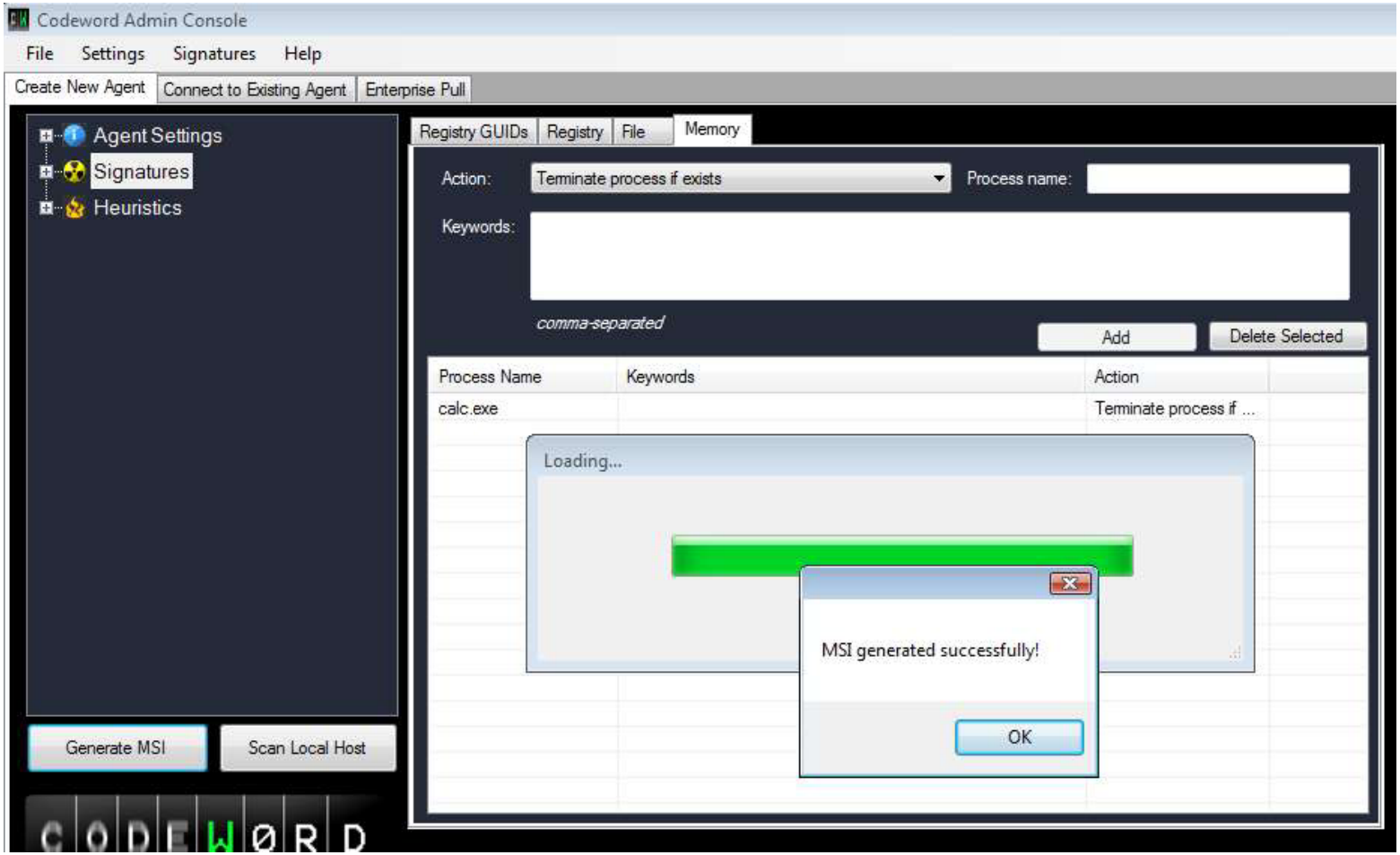
# Defining signatures



# Selecting Heuristics



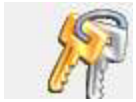
# Generate it!

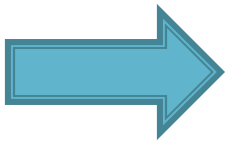

Codeword Admin Console
File
Settings
Signatures
Help
Create New Agent
Connect to Existing Agent
Enterprise Pull
Agent Settings
Signatures
Heuristics
Registry GUIDs
Registry
File
Memory
Action:
Terminate process if exists
Process name:
Keywords:
comma-separated
Add
Delete Selected
Process Name
Keywords
Action
calc.exe
Terminate process if ...
Loading...
MSI generated successfully!
OK
Generate MSI
Scan Local Host
CODEWORD

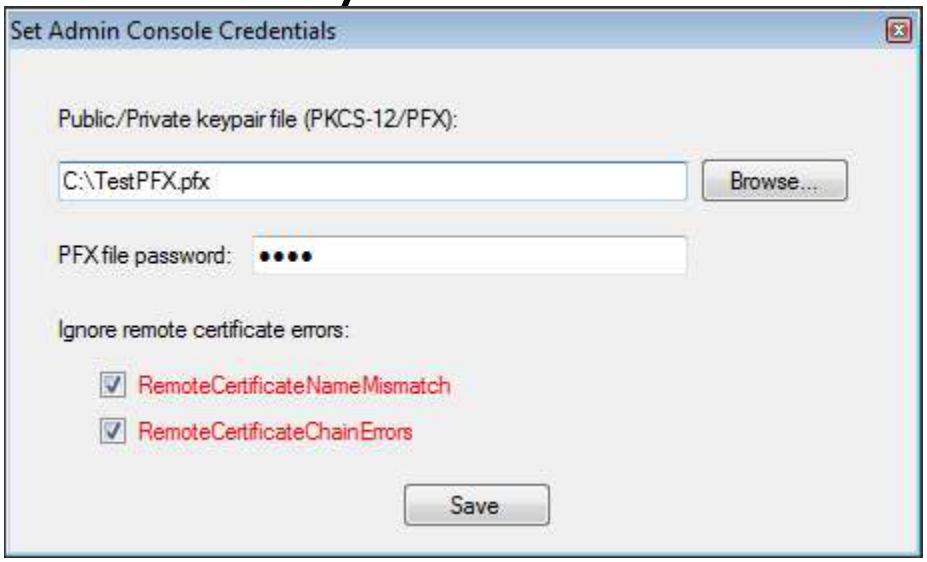
# Step 2: Connect/Scan/Analyze
## Enterprise and Remote Control Modes

# Connecting to an agent

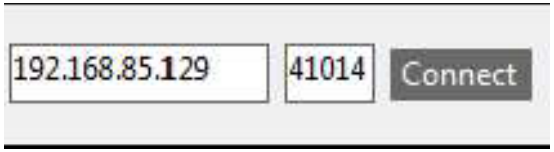
1. Specify admin console keys



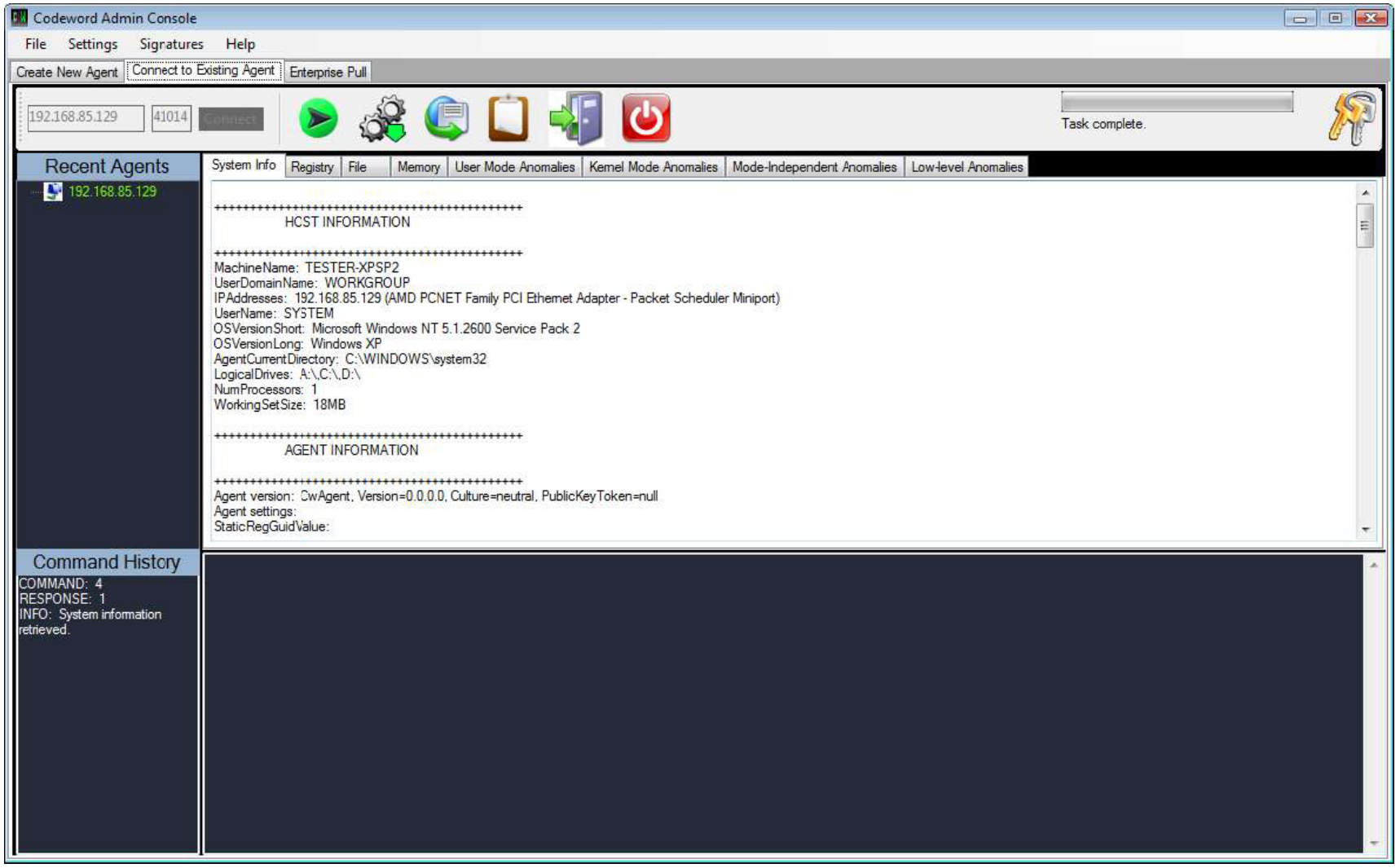




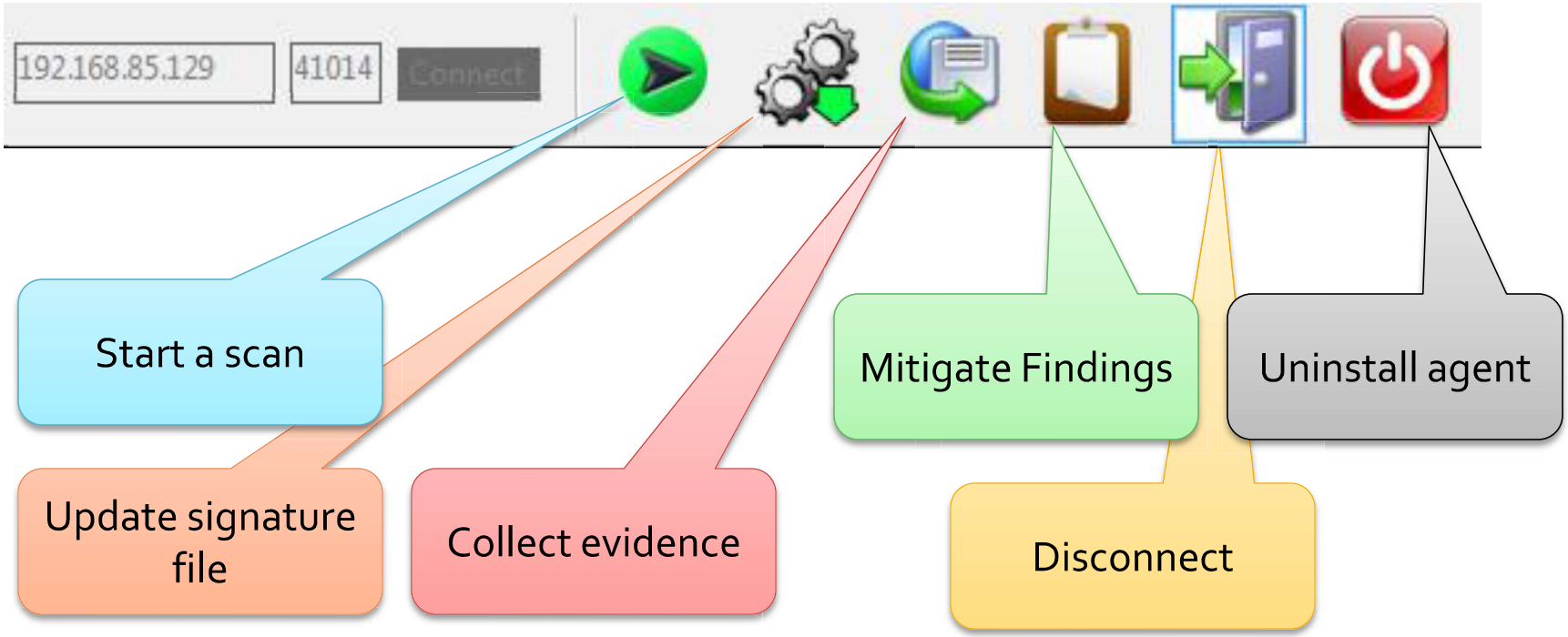

2. Click connect!



# ..we are connected



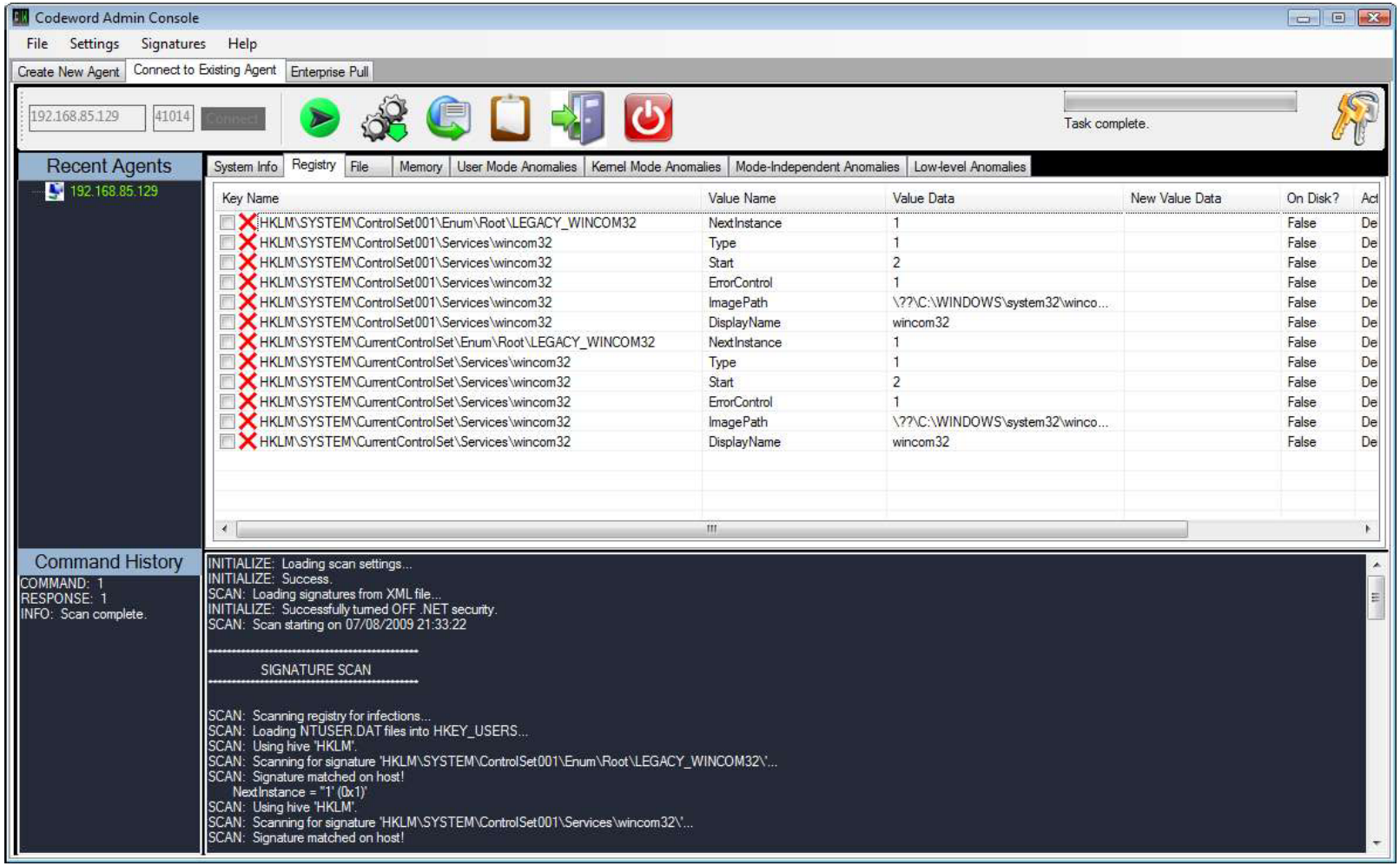
# The Toolbar


192.168.85.129
41014
Connect
Start a scan
Update signature file
Collect evidence
Mitigate Findings
Disconnect
Uninstall agent

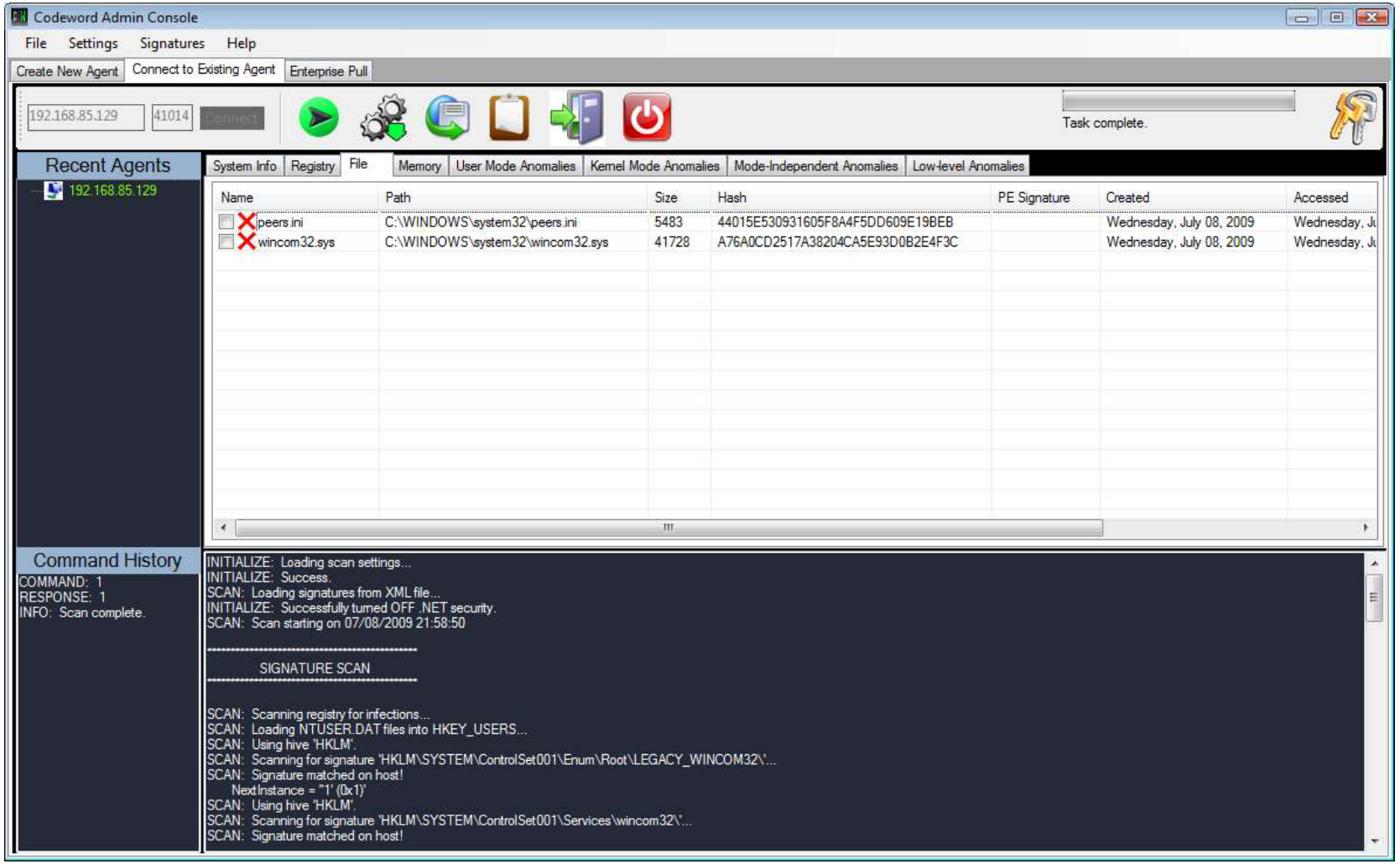
# Issue a scan

- Click the big green "PLAY" button
- Issues a command to the agent to begin scanning with whatever signature file it has
- Scan as many times as you like; change signatures by uploading new signatures file

# Storm Worm Results: Registry

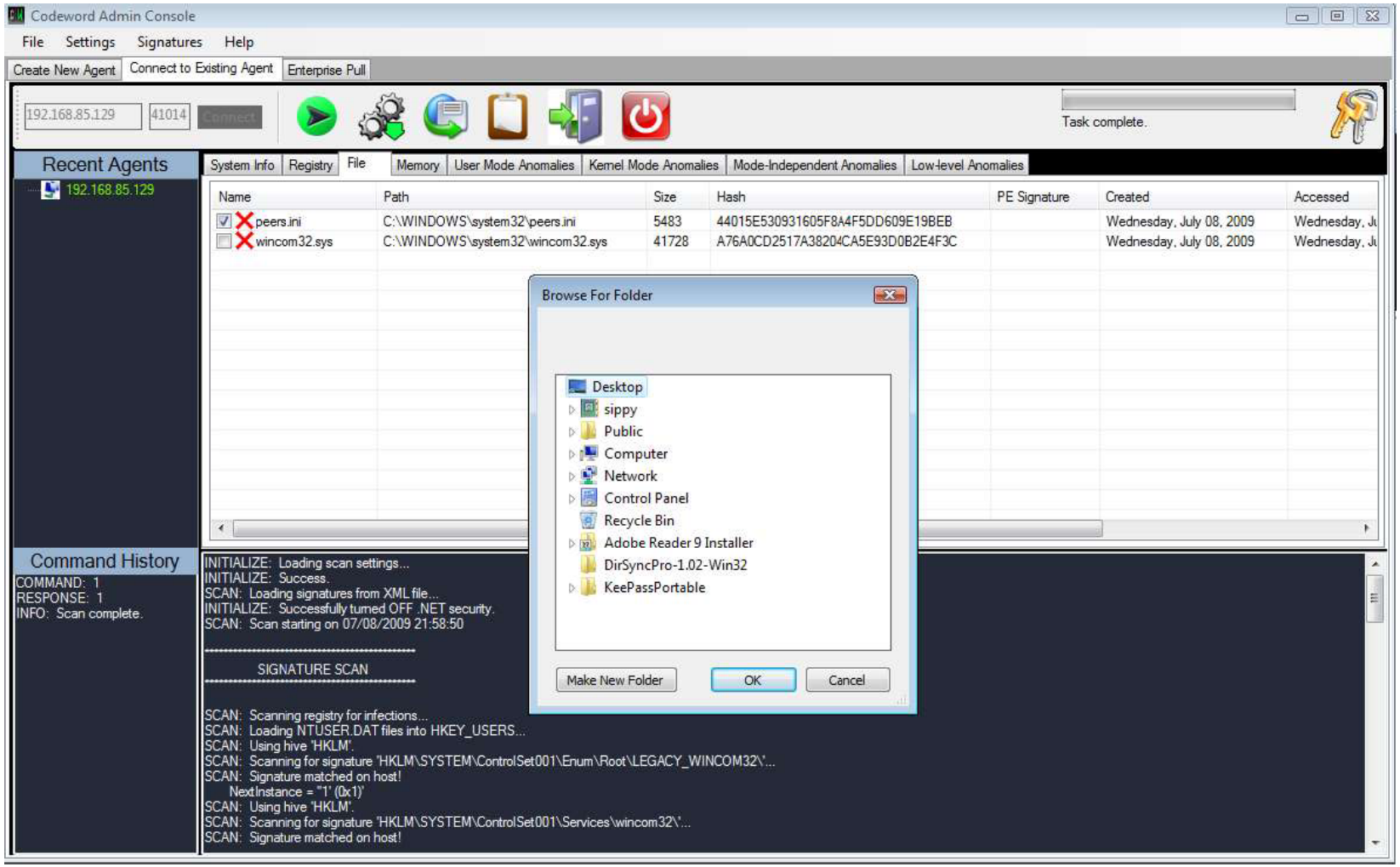


# Storm Worm Results: File

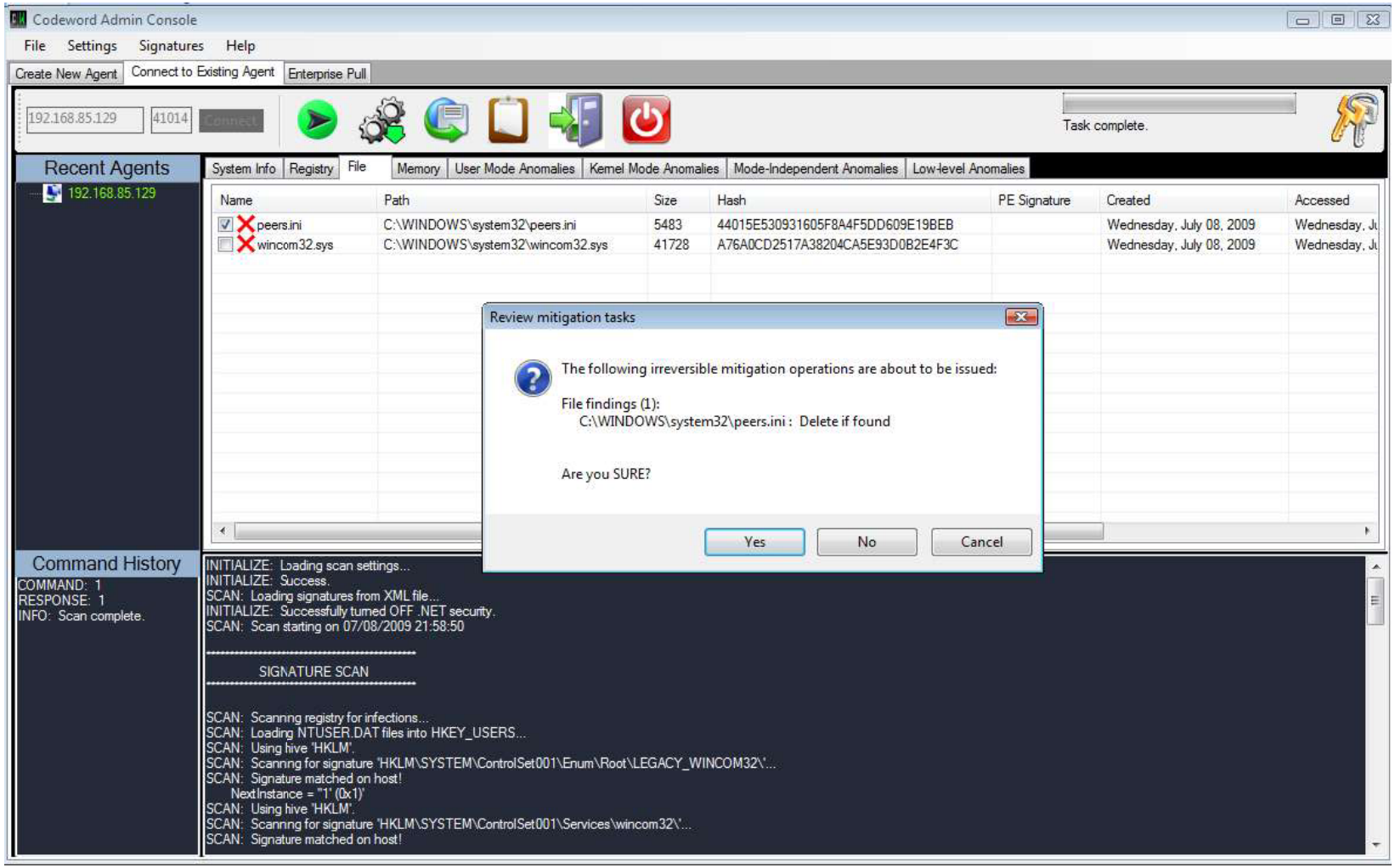


# Step 3: Collect and Mitigate
## Enterprise and Remote Control Modes

# Collect


Codeword Admin Console
File Settings Signatures Help
Create New Agent
Connect to Existing Agent
Enterprise Pull
192.168.85.129
41014
Connect
Task complete.
Recent Agents
192.168.85.129
System Info
Registry
File
Memory
User Mode Anomalies
Kernel Mode Anomalies
Mode-Independent Anomalies
Low-level Anomalies
Name
Path
Size
Hash
PE Signature
Created
Accessed
peers.ini
C:\WINDOWS\system32\peers.ini
5483
44015E530931605F8A4F5DD609E19BEB
Wednesday, July 08, 2009
wincom32.sys
C:\WINDOWS\system32\wincom32.sys
41728
A76A0CD2517A38204CA5E93D0B2E4F3C
Wednesday, July 08, 2009
Browse For Folder
Desktop
sippy
Public
Computer
Network
Control Panel
Recycle Bin
Adobe Reader 9 Installer
DirSyncPro-1.02-Win32
KeePassPortable
Make New Folder
OK
Cancel
Command History
COMMAND: 1
RESPONSE: 1
INFO: Scan complete.
INITIALIZE: Loading scan settings...
INITIALIZE: Success.
SCAN: Loading signatures from XML file...
INITIALIZE: Successfully turned OFF .NET security.
SCAN: Scan starting on 07/08/2009 21:58:50
SIGNATURE SCAN
SCAN: Scanning registry for infections...
SCAN: Loading NTUSER.DAT files into HKEY_USERS...
SCAN: Using hive 'HKLM'.
SCAN: Scanning for signature 'HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_WINCOM32\'...
SCAN: Signature matched on host!
NextInstance = "1" (0x1)'
SCAN: Using hive 'HKLM'.
SCAN: Scanning for signature 'HKLM\SYSTEM\ControlSet001\Services\wincom32\'...
SCAN: Signature matched on host!

# Mitigate


Codeword Admin Console
File Settings Signatures Help
Create New Agent
Connect to Existing Agent
Enterprise Pull
192.168.85.129
41014
Connect
Task complete.
Recent Agents
192.168.85.129
System Info
Registry
File
Memory
User Mode Anomalies
Kernel Mode Anomalies
Mode-Independent Anomalies
Low-level Anomalies
Name
Path
Size
Hash
PE Signature
Created
Accessed
peers.ini
C:\WINDOWS\system32\peers.ini
5483
44015E530931605F8A4F5DD609E19BEB
Wednesday, July 08, 2009
wincom32.sys
C:\WINDOWS\system32\wincom32.sys
41728
A76A0CD2517A38204CA5E93D0B2E4F3C
Wednesday, July 08, 2009
Review mitigation tasks
The following irreversible mitigation operations are about to be issued:
File findings (1):
C:\WINDOWS\system32\peers.ini : Delete if found
Are you SURE?
Yes
No
Cancel
Command History
COMMAND: 1
RESPONSE: 1
INFO: Scan complete.
INITIALIZE: Loading scan settings...
INITIALIZE: Success.
SCAN: Loading signatures from XML file...
INITIALIZE: Successfully turned OFF .NET security.
SCAN: Scan starting on 07/08/2009 21:58:50
SIGNATURE SCAN
SCAN: Scanning registry for infections...
SCAN: Loading NTUSER.DAT files into HKEY_USERS...
SCAN: Using hive 'HKLM'.
SCAN: Scanning for signature 'HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_WINCOM32\'...
SCAN: Signature matched on host!
NextInstance = "1" (0x1)'
SCAN: Using hive 'HKLM'.
SCAN: Scanning for signature 'HKLM\SYSTEM\ControlSet001\Services\wincom32\'...
SCAN: Signature matched on host!

# Mitigate (2)

| Name | Path | Size | Hash |
|---|---|---|---|
| peers.ini | C:\WINDOWS\system32\peers.ini | 5483 | 44015E530931605F8A4F5DD609E19BEB |
| wincom32.sys | C:\WINDOWS\system32\wincom32.sys | 41728 | A76A0CD2517A38204CA5E93D0B2E4F3C |

# Fire-and-forget Mode

# What's reported?

- A password-protected, encrypted (AES 256) Zip archive containing:
  - Infection summary report
  - Mitigation report
  - All collected malware binaries and evidence
  - A detailed run log

# Video Demos

# Demo #1: Storm Worm

- GOAL:
  - Understand how to define registry, disk and memory signatures to detect user-mode malware
- SCENARIO:
  - VM Guest infected with Storm worm
- OBJECTIVES:
  - Deploy agent using Remote Control mode
  - Examine malware footprints

# Demo #2: TcpIrpHook

- GOAL:
  - Understand how Codeword heuristics help catch kernel malware (and anti-virus)
- SCENARIO:
  - VM Guest infected with kernel-mode rootkit TcpIrpHook
- OBJECTIVES:
  - Deploy agent using Remote Control mode
  - Scan with Driver IRP hook heuristic

# Conclusions

# Possible Limitations

- Software licensing costs can be prohibitive
  - These costs are outweighed by user productivity
  - "renting" the software may be a cost-effective solution
- Some challenges that plague traditional methods also impact RETRI:
  - Disorganized networks, lack of funding, lack of mgmt-level support, lack of resources, etc.
  - Assumptions made early on have cumulative impact later on:
    - Availability of backups
    - COOP readiness
    - Date and scope of infection

# Final Thoughts

- Preparation is key to ensuring services are restored quickly
  - Know your network and critical services
  - Ensure backups exist
  - Have hardware / software ready
- Keeping services up significantly reduces the cost of recovery
- Remember: User downtime costs 3 times as much as the actual cleanup

# Thanks for coming!!

Email us
Mike.A.Murphy@gmail.com
AaronLemasters@yahoo.com

Website:
www.hexsec.com
www.code-word.org