

Telesis/Endeavor

Moving Target Defense

Will Hickie

Will.Hickie@endeavorsystems.com

Question

- Who likes getting calls from Telemarketers?



Telesis/Endeavor

Public Interfaces



555-1212



Public Interface Obfuscation



555-1212
556-1212
525-1282
472-6519
832-0194
634-0973
203-1337



Public Interface Obfuscation



555-1212
556-1212
525-1282
472-6519
832-0194
634-0973
203-1337



472-6519



472-6519



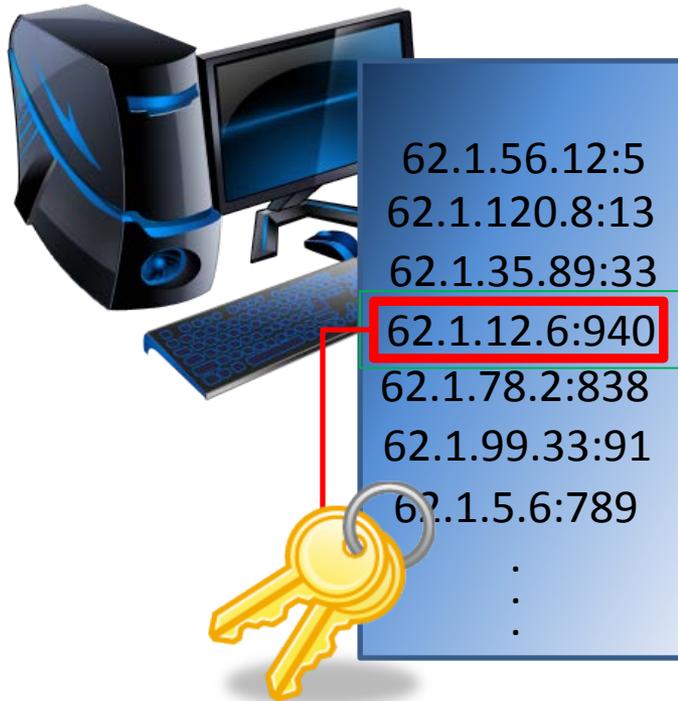
555-1212



472-6519



Public Interface Obfuscation



62.1.12.6:940



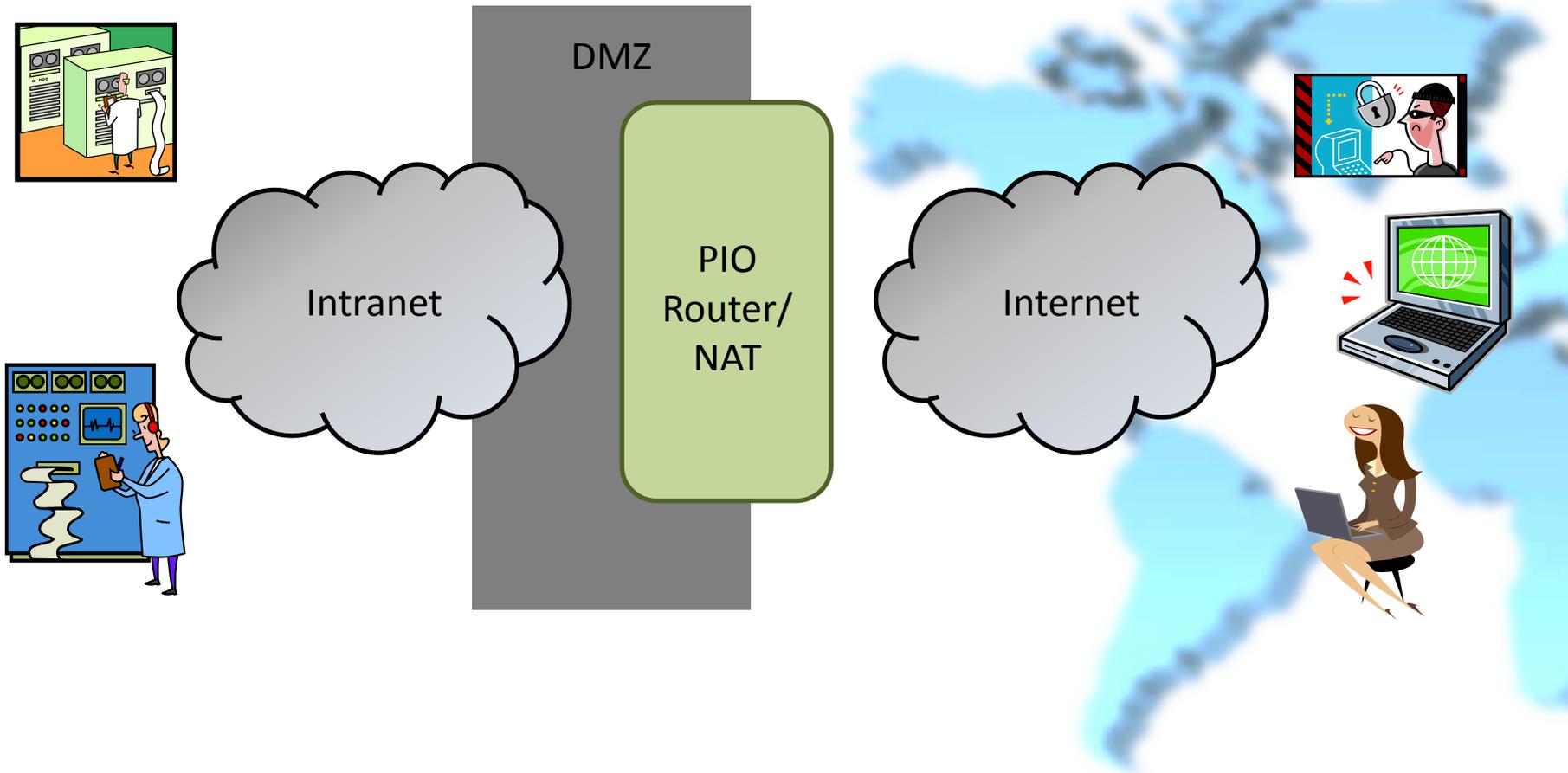
62.1.12.6:940



62.1.12.6:940



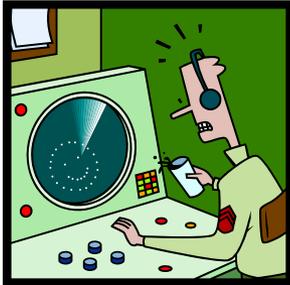
Public Interface Obfuscation



Public Interface Obfuscation



No more 'Phishing'



Port scanning stops working— ports are always changing!

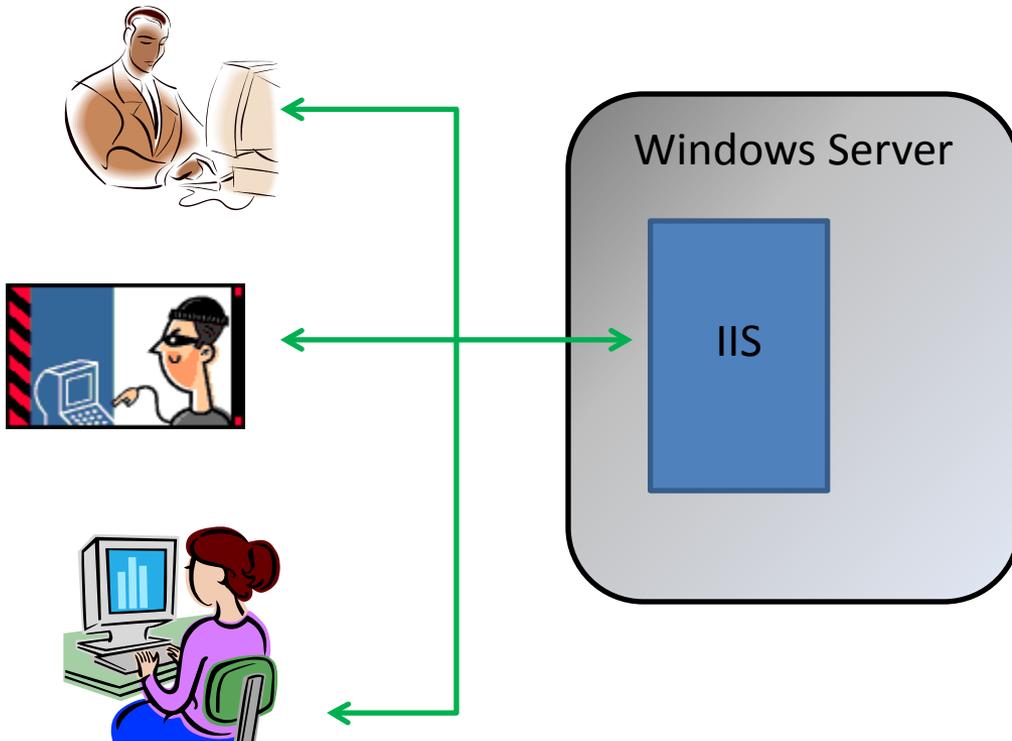


Window of opportunity very small for attackers as locations constantly shift.

But what if...?

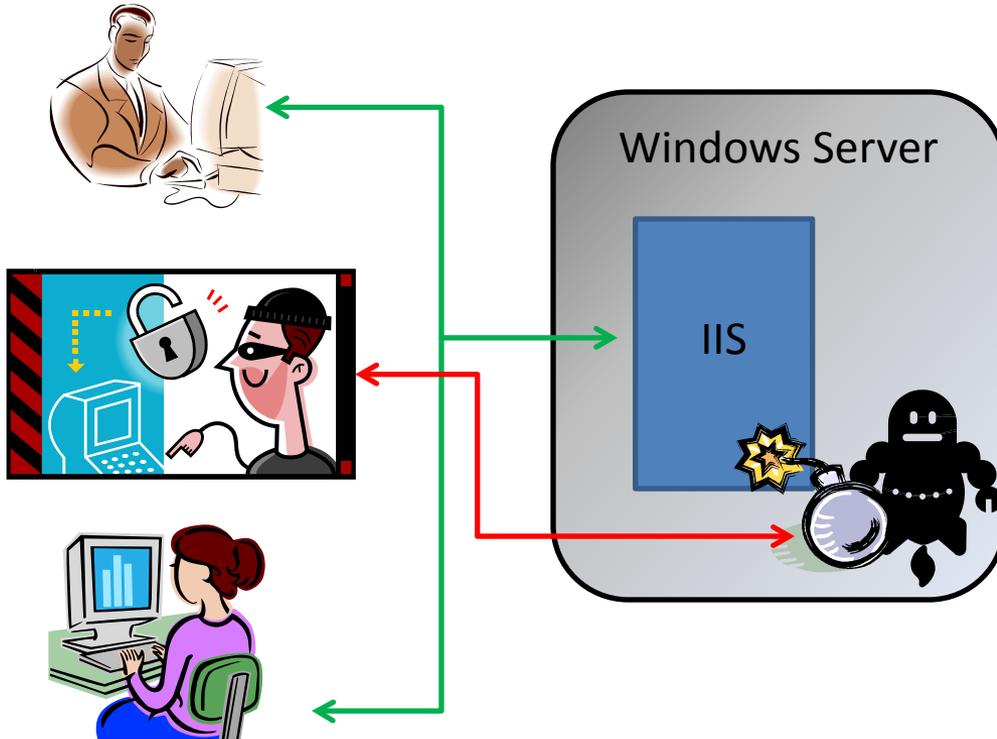


Live Service Migration



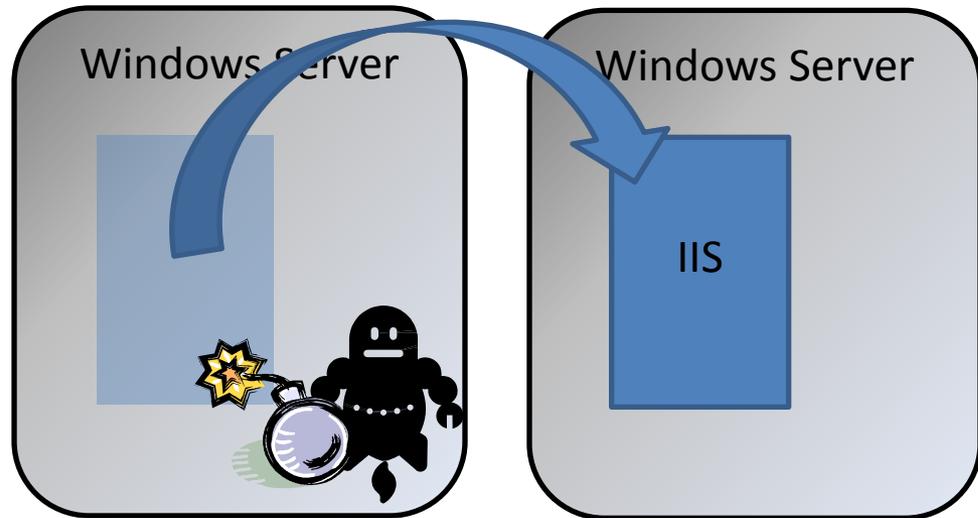
Normal operation:
- Everyone using the web server.

Live Service Migration



Abnormal operation:
- Someone/something bypasses web server.

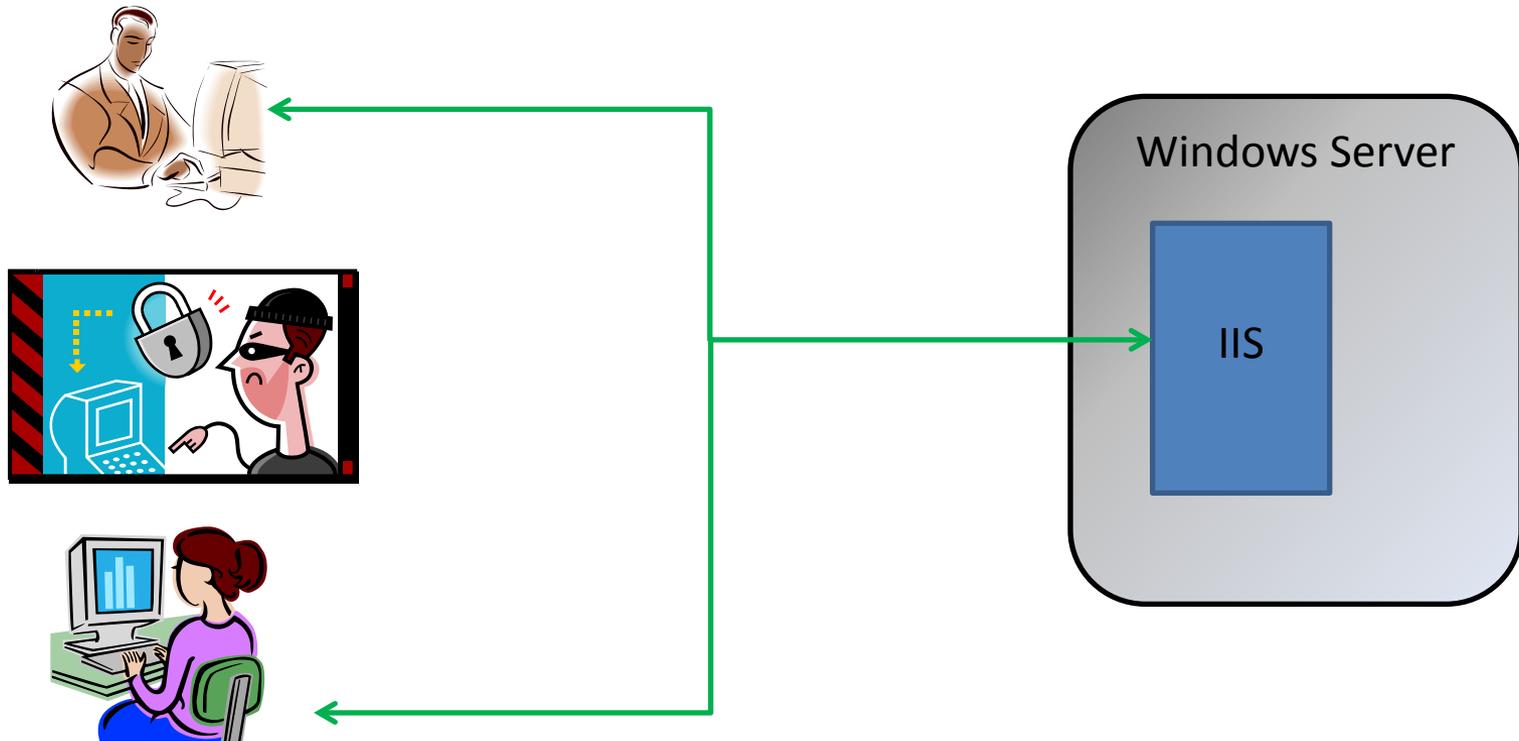
Live Service Migration



Live Service Migration:

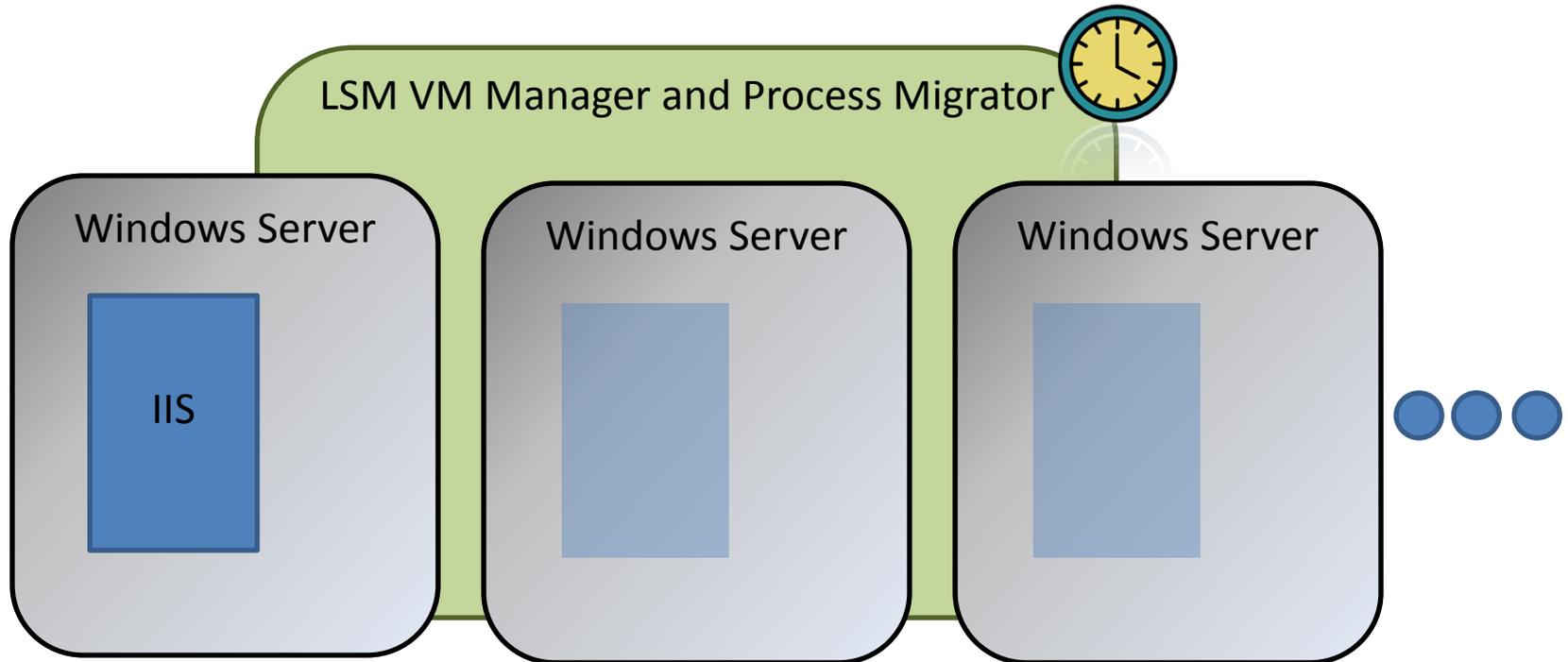
- Machine suspended, process migrated.

Live Service Migration



Normal operation:
- Everyone using the web server.

Live Service Migration



- At regular intervals, services are migrated.
- LSM interrupts the attackers mission, not the initial attack.
- Ordinary legitimate use carries on

Telesis/Endeavor Moving Target

- Public Interface Obfuscation
 - Protects the front door
 - Everything coming in is 'pre' authenticated
 - Almost impossible to ID a system
 - Very difficult to exploit a service
- Live Service Migration:
 - Protects the services
 - Prevents exploits from persisting
 - Stops root-kits and malware from working

Telesis/Endeavor Moving Target

- Questions?

Will Hickie

Will.Hickie@endeavorsystems.com