

Table of Contents

Table of Contents.....	2
Inter Process Connection Introduction.....	4
1. Banking Trojan Coordinating Information Collection.....	5
2. Ransomware Sharing Encryption Keys.....	5
3. Remote Access Trojans (RATs) Managing System Resources.....	6
4. Modular Malware Framework Passing Exploits to a Loader.....	6
5. Spyware Collecting and Aggregating User Data.....	6
6. Credential Theft Using Token Injection.....	6
7. Botnet Coordination and Distributed Task Processing.....	6
8. Process Hollowing and Code Injection.....	7
9. Credential Dumping and Memory Scraping in POS Malware.....	7
10. Adware or PUP (Potentially Unwanted Program) Persistence and Self-Restart.....	7
Mutex.....	7
How Mutex Works.....	8
Why Mutexes Are Used.....	8
Mutexes in Malware Development.....	8
Key Concepts and Windows API Functions.....	9
Pipe.....	11
Mapped File.....	15
Registry.....	20
Shared Memory.....	30
Message Queues.....	33
Implementing Message Queues for Malware IPC.....	34
Explanation:.....	35
Advanced Tips.....	35
Clipboard.....	36
Explanation of Code.....	39
Potential Malware Applications.....	39
Semaphores.....	40
Explanation of Code.....	42
Potential Malware Applications.....	42
Proof of Concept.....	43
Events.....	43
Key Features:.....	43
Basic Usage:.....	44
.....	47
Exercise.....	47
Requirements:.....	47
Goals:.....	48
Conclusions.....	48

