Erratum to:

Integrating Cyber-D&D into Adversary Modeling for Active Cyber Defense

Frank J. Stech, Kristin E. Heckman, and Blake E. Strom

S. Jajodia et al. (eds.), *Cyber Deception*
DOI 10.1007/978-3-319-32699-3

DOI 10.1007/978-3-319-32699-3_13

The original version of this book was inadvertently published with an incorrect Table 3 in Chapter 1. The correct Table is as follows:

Table 3 MITRE ATT&CK matrix™—overview of tactics and techniques described in the ATT&CK model

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Host Enumeration	Lateral Movement	Execution	C2	Exfiltration
Legitimate Credentials			Credential Dumping	Account enumeration	Application deployment software	Command Line	Commonly used port	Automated or scripted exfiltration
Accessibility Features		Binary Padding	Credentials in Files	File system enumeration	Exploitation of Vulnerability	File Access	Comm through removable media	Data compressed
AddMonitor		DLL Side-Loading	Network Sniffing	Group permission enumeration	Logon scripts	PowerShell	Custom application layer protocol	Data encrypted
DLL Search Order Hijack		Disabling Security Tools	User Interaction	Local network connection enumeration	Pass the hash	Process Hollowing	Custom encryption cipher	Data size limits
Edit Default File Handlers		File System Logical Offsets		Local networking enumeration	Pass the ticket	Registry	Data obfuscation	Data staged
New Service		Process Hollowing		Operating system enumeration	Peer connections	Rundll32	Fallback channels	Exfil over C2 channel
Path Interception		Indicator blocking on host		Owner/User enumeration	Remote Desktop Protocol	Scheduled Task	Multiband comm	Exfil over alternate channel to C2 network
Scheduled Task		Indicator removal from tools		Process enumeration	Windows management instrumentation	Service Manipulation	Multilayer encryption	Exfil over other network medium
Service File Permission Weakness		Indicator removal from host		Security software enumeration	Windows remote management	Third Party Software	Peer connections	Exfil over physical medium
Shortcut Modification		Masquerading		Service enumeration	Remote Services		Standard app layer protocol	From local system
BIOS	Bypass UAC	NTFS Extended Attributes		Window enumeration	Replication through removable media		Standard non-app layer protocol	From network resource
Hypervisor Rootkit	DLL Injection	Obfuscated Payload			Shared webroot		Standard encryption cipher	From removable media
Logon Scripts	Exploitation of Vulnerability	Rootkit			Taint shared content		Uncommonly used port	Scheduled transfer
Master Boot Record		Rundll32			Windows admin shares			
Mod. Exist'g Service		Scripting						
Registry Run Keys		Software Packing						
Serv. Reg. Perm. Weakness								
Windows Mgmt Instr. Event Subsc.								
Winlogon Helper DLL								

Approved for Public Release; Distribution Unlimited. Case Number 15-1288
MITRE

The online version of the original chapter can be found at
http://dx.doi.org/10.1007/978-3-319-32699-3_1