Matrix PDF

Matrix

Kill Chain / Tactics	Recruitment /Turning point	Search /Reconnaisance	Defense Evasion	Initiate		Execution /Action		Aftermath
				Data Collection	Weaponise	Exfiltrate	Impact	
Techniques	Malicious Recruitment	Searching through data not application to job	Deleting Logs/IT evidence	Unauthorised access • Accessing services with correct creds (but shouldn't have access) • Password theft	Download malware	Leveraging remote access	Deletion of data	Gloating
	Make Contact	Contacting people for info/help not applicable to job	Destroying physical evidence	Coercing contacts	Writing malicious code	External technical exfiltration • Dropbox • Email • USB/CD	Editing critical data	Frivilous purchases
	Exposed to temptation (Unreviewed/regulated processes)	Applying for promotions/job changes	Impersonation/Masquerading	Keylogger	Unauthorised access	External physical exfiltration • Printing large amounts • Taking photos • Memorising • Writing down	Attack availability	Last minute /unannounced holidays/travel?
	Surprising Change in Behaviour	Suspicious requests not compliant with company policy	Requesting staff overlook responsibilities	Collecting data in a centralized place	Installing malicious code		Transfer of money	Surprise Resignation
	Unprofessional Behaviour	Malicious unapproved access to other systems	Defensive Collusion	Authorised Access	Testing Malicious Code		Extortion	Refuses promotion /team transfer
	Resignation/Surprise Resignation	Online research on how to build malicious code	Exploit Turbulence		Privilege Escalation		Public release of data	Created a competing company
	Disgruntlement				Abuse of process			Attempt to steal customers from the company
	Dismissal							Confession
	Change in personal life							

Techniques to Examples

Recruitment/Turning point

Techniques	Examples / Procedures	Citations
Malicious Recruitment	From foreign government	Cert Guide to Insider Threats: Theft of IP 4
	Recruited by a competing firm	Cert Guide to Insider Threats: Fraud Case 4
	Recruited by malicious outsider	Cert Guide to Insider Threats: Fraud 6 Cert Guide to Insider Threats: Fraud 8

	Persuaded by disgruntled coworkers	Office Space
Make Contact	Contacting foreign government offering Services	Geoffrey Prime
	Offer services to competing companies	Cert Guide to Insider Threats: Theft of IP 2
Disgruntlement	Downgrade of responsibilities e.g. Company increasing in size and original employee losing relative importance in company e.g. being changed from full-time to part-time, or from employee to consultant /contractor with fewer benefits	Cert Guide to Insider Threats: Sabotage 8 Cert Guide to Insider Threats: Sabotage 15
	Dispute with management	Cert Guide to Insider Threats: Sabotage 7 Cert Guide to Insider Threats: Sabotage 12 Cert Guide to Insider Threats: Sabotage 15
	Dispute with colleagues (verbal/physical assaults; threats)	Cert Guide to Insider Threats: Sabotage 8 Cert Guide to Insider Threats: Sabotage/Fraud 2 Cert Guide to Insider Threats: Sabotage/Fraud 3
	Blackmailing/Threatening to sue company	Cert Guide to Insider Threats: Sabotage 7
	Contract not renewed/rejected	Cert Guide to Insider Threats: Sabotage 6
	Finding out in advance to be terminated	Cert Guide to Insider Threats: Sabotage 11 Office Space
	Poor working conditions: • Overworked/forced to work overtime • Poor work environments	Office Space
	Security Concerns raised and ignored. Disgruntled employee felt his security concerns were being ingnored	Cert Guide to Insider Threats: Miscellaneous 4
	Dismissed/Fired/Made Redundant	Cert Guide to Insider Threats: Sabotage 1 Cert Guide to Insider Threats: Miscellaneous 1 Cert Guide to Insider Threats: Sabotage 8 Cert Guide to Insider Threats: Sabotage 4 Cert Guide to Insider Threats: Malicious 6
Exposed to temptation (Unreviewed/regulated processes)	Suspicious interest in a competitor	Cert Guide to Insider Threats: Theft of IP 1
	Accidentally discovers access to assets	Office Space
Change in personal life	Financial difficulties	Cert Guide to Insider Threats: Fraud 9
IOC	**Examples**	**Citations**

Unprofessional behaviour	Frequent tardiness	Cert Guide to Insider Threats: Sabotage 11 Office Space
	Undue absence/sickness leaves	Cert Guide to Insider Threats: Sabotage 11 Office Space
	Suddenly refusing to help colleagues in their work.	Cert Guide to Insider Threats: Sabotage 8
	Trying to discredit others, e.g. writing faulty programs to make colleagues look bad	Cert Guide to Insider Threats: Sabotage 8
	Generic acting out	Office Space
Surprising change in behaviour	Unexplained change in performance	Cert Guide to Insider Threats: Fraud 11

Search/Reconnaissance

Techniques	Examples / Procedures	Citation
Searching through data not applicable to job	Email system (e.g. searching for executives, directors, HR emails)	Cert Guide to Insider Threats: Miscellaneous 1
Contacting people for info/help not applicable to job	Terminated employee emailing present emloyees	Cert Guide to Insider Threats: Miscellaneous 1
	Requesting critical data. Requesting backup of critical company system process (e.g. manufacturing process)	Cert Guide to Insider Threats: Sabotage 8
Suspicious requests not compliant with company policy	Asking colleagues not to perform due diligence	Cert Guide to Insider Threats: Fraud Case 3
	Requesting perms not needed for job	Cert Guide to Insider Threats: Fraud 10
Malicious unapproved access to other systems	Installed malware on coworker's machines	Cert Guide to Insider Threats: Fraud 4
	Accessed servers with root password using password cracker	Cert Guide to Insider Threats: Miscellaneous 4
	Looking around on other servers for information	Snowden
	Using a colleague's credentials	Cert Guide to Insider Threats: Fraud 12
Applying for promotions/job changes	Applied for jobs at high tech companies	Cert Guide to Insider Threats: Theft of IP 4

Defence Evasion

Techniques	Examples / Procedures	Citation
Requesting staff overlook responsibilities	Asking colleagues not to perform due diligence	Cert Guide to Insider Threats: Fraud Case 3
Destroying physical evidence	Shredding paper	Enron Barclays
	Arson	Office Space
Deleting logs/IT evidence	Deleting temp files on Company Computer (e.g. BYOD laptop)	Cert Guide to Insider Threats: Theft of IP 1
	Deleting bash logs	Cert Guide to Insider Threats: Miscellaneous 6
	Deleting database logs	Cert Guide to Insider Threats: Fraud 11
	Reformat backups	Cert Guide to Insider Threats: Fraud 11

	Wiped laptops	Uber/Google Lawsuit
Hiding Files	Changing an incriminating computer file into hidden mode	Insider Threat Protecting the Enterprise: Case Study Customers with Access Become Insiders
Impersonation /Masquerading	Trying to frame a colleague with whom insider has conflict	Cert Guide to Insider Threats: Sabotage 1
	Using computer account which share name of other employee to send email	Cert Guide to Insider Threats: Sabotage 1
	Modifying favourably the payroll of a colleague	Cert Guide to Insider Threats: Sabotage 1
	Use colleague's computers & accounts	Cert Guide to Insider Threats: Fraud 8 Cert Guide to Insider Threats: Fraud 12
Exploit Turbulence	Use the fact work is behind schedule to avoid discovery	Office Space
Defensive Collusion	Separation of task such that one person doesn't do too much by themselves	Cert Guide to Insider Threats: Fraud 12 Office Space

Initiate

Data Collection

Techniques	Examples / Procedures	Citation
Collecting data in a centralized place	Storing cracked passwords on a company's server	Cert Guide to Insider Threats: Sabotage 10
	Storing cracked password on a company's laptop	Insider Threat Protecting the Enterprise: Case Study Customers with Access Become Insiders
	Write programs to steal data from DB	Cert Guide to Insider Threats: Miscellaneous Case 3
	Mass copying of data onto physical media	Chelsea Manning Snowden Insider Threat Protecting the Enterprise: Case Study Customers with Access Become Insiders
	Amassing data you use as part of your job	Uber/Google Lawsuit Apple Insider
Unauthorised access • Accessing services with correct creds (but shouldn't have access) • Password theft	Sharing passwords with colleagues	Cert Guide to Insider Threats: Fraud 7
	Compromising other's credentials to masquerade as them for access	Cert Guide to Insider Threats: Miscellaneous 6
	Accessing company's system with knowledge of default password	Insider Threat Protecting the Enterprise: Case Study Former Employee Eavesdrops on Voice Mail for Competitive Advantage
Coercing contacts	Attempted to recruit others to provide data	Cert Guide to Insider Threats: Theft of IP 4
Keylogger	Keylogger in Malware collected confidential information	Cert Guide to Insider Threats: Fraud 4
Authorised access	Making authorised one off data requests for information you have no need to access	Cert Guide to Insider Threats: Fraud 6

Weaponise

Techniques	Examples / Procedures	Citation

Download malware		Cert Guide to Insider Threats: Fraud 4
Writing malicious code		Cert Guide to Insider Threats: Sabotage 4 Office Space
Installing malicious code	Infecting machines through a standard upgrade	Cert Guide to Insider Threats: Sabotage 3 Office Space
	Installing malware on own computer	Cert Guide to Insider Threats: Fraud 4
	Installing a password-cracking software	Cert Guide to Insider Threats: Sabotage 10 Cert Guide to Insider Threats: Misc case 4 Insider Threat Protecting the Enterprise: Case Study Customers with Access Become Insiders
	Installing a scheduled job that performs automatically the data exfiltration on a periodic basis	Cert Guide to Insider Threats: Sabotage 10
	Installed logic bombs on network	Cert Guide to Insider Threats: Sabotage 6
Testing malicious code	Testing code shortly prior to termination	Cert Guide to Insider Threats: Sabotage 8
	Testing logic bomb on network	Cert Guide to Insider Threats: Sabotage 8
Unauthorised access	Using credentials after leaving the company	Cert Guide to Insider Threats: Sabotage 5
Privilege Escalation	Creating an administrator account	Cert Guide to Insider Threats: Sabotage 10
	Using perms no longer relevant to role that had previously been granted and not revoked	Cert Guide to Insider Threats: Fraud 9
	Creating faking credentials in the system	Cert Guide to Insider Threats: Sabotage/Fraud 2
	Using a colleagues credentials	Cert Guide to Insider Threats: Fraud 12
Abuse of process	Preparing a fraudulent money transfer Submitting a payment request that will be subsequently maliciously modified	Cert Guide to Insider Threats: Fraud 7
	Submitted legitimate requests fraudulently Submitted fake requests for drivers licences	Cert Guide to Insider Threats: Fraud 6

Execution/Action

Exfiltrate

Techniques	Examples / Procedures	Citation
External technical exfiltration • Dropbox • Email • USB/CD • Company BYOD (Laptop)	Copying code to removable media	Cert Guide to Insider Threats: Sabotage 3 Cert Guide to Insider Threats: Fraud 3 Cert Guide to Insider Threats: Theft of IP 1
	Copying code to CDs	Cert Guide to Insider Threats: Theft of IP 6 Chelsea Manning
	Email Journalists	Cert Guide to Insider Threats: Sabotage 7
	Malware exfiltrated data from network	Cert Guide to Insider Threats: Fraud 4

	Email self data	Tesla/Zoox
External physical exfil • Printing large amounts • Taking photos • Memorising • Writing down	Printing documents	Reality Winner
Leveraging remote access		Cert Guide to Insider Threats: Theft of IP 3 Cert Guide to Insider Threats: Sabotage 3 Cert Guide to Insider Threats: Fraud 3
	Leveraging remote access after termination of contract	Cert Guide to Insider Threats: Sabotage 10 Insider Threat Protecting the Enterprise: Case Study Former Employee Eavesdrops on Voice Mail for Competitive Advantage

Impact

Techniques	Examples / Procedures	Citation
Deletion of data	Detonating Logic Bomb to delete data	Cert Guide to Insider Threats: Sabotage 2 Cert Guide to Insider Threats: Sabotage 3
	Deleting critical IT programs/data	Cert Guide to Insider Threats: Sabotage 8 Cisco Webex
	Deleting compensation documents	Cert Guide to Insider Threats: Sabotage 1
Attack availability	Detonating Logic Bomb to attack availability	Cert Guide to Insider Threats: Sabotage 5 Cert Guide to Insider Threats: Sabotage 6
	Shutting down company operations Hitting "Emergency power off" button (e.g. in a plant)	Cert Guide to Insider Threats: Sabotage 9
Editing critical data	Changing status of applications eg for asylum/welfare	Cert Guide to Insider Threats: Fraud 8 Cert Guide to Insider Threats: Fraud 9
	Changed state lottery records	Cert Guide to Insider Threats: Fraud 11
	Changing delivery address	Cert Guide to Insider Threats: Fraud 12
	Editing company codebase Removed technical changes from code	Cert Guide to Insider Threats: Miscellaneous 6 Tesla
	Sabotaging colleagues' projects	Cert Guide to Insider Threats: Sabotage 8
Transfer of money	Using a privileged account to edit the vendor details in a payment e.g. editing details in favour of a relative/friend and changing back to original data after payment is made	Cert Guide to Insider Threats: Fraud 7
	Use malicious code to perform minor transfers of money	Office Space
	Fake purchase orders into personal bank account	Cert Guide to Insider Threats: Fraud 10

Extortion		Cert Guide to Insider Threats: Sabotage 4
Produce fraudulent services	Produced fake drivers licences for people	Cert Guide to Insider Threats: Fraud 6
Public release of data	Publish data on website	Cert Guide to Insider Threats: Sabotage 23 Morrions
	Give data to the media	Snowden

Aftermath

Techniques	Examples / Procedures	Citation
Gloating	Bragged about his actions	Cert Guide to Insider Threats: Miscellaneous case 4
Frivolous purchases		Aldrich Ames
Last minute/unannounced holidays/travel?		Office Space
Surprise Resignation		Cert Guide to Insider Threats: IP Theft 1
Created a competing company	Created a competing company with stolen data	Cert Guide to Insider Threats: IP Theft 4 Uber/Google Lawsuit
	Recruiting several key employees	Uber/Google Lawsuit Insider Threat Protecting the Enterprise: Case Study Eastman Kodak Corporation Is Victimized by a Retiree
Attempt to steal customers from the company	Stolen data used to steal customers	Cert Guide to Insider Threats: Fraud 4
Attempting to sell proprietary information to competitors	Competitor receiving an email attempting to sell them stolen information	Insider Threat Protecting the Enterprise: Case Study Loss of "Buy-In" Causes Employee to Turn Against His Company Insider Threat Protecting the Enterprise: Case Study Eastman Kodak Corporation Is Victimized by a Retiree
Confession	Feels guilt and confesses	Office Space
	Confesses upon accusation	Apple Insider
Refuses promotion/team transfer		India RTO Inspectors