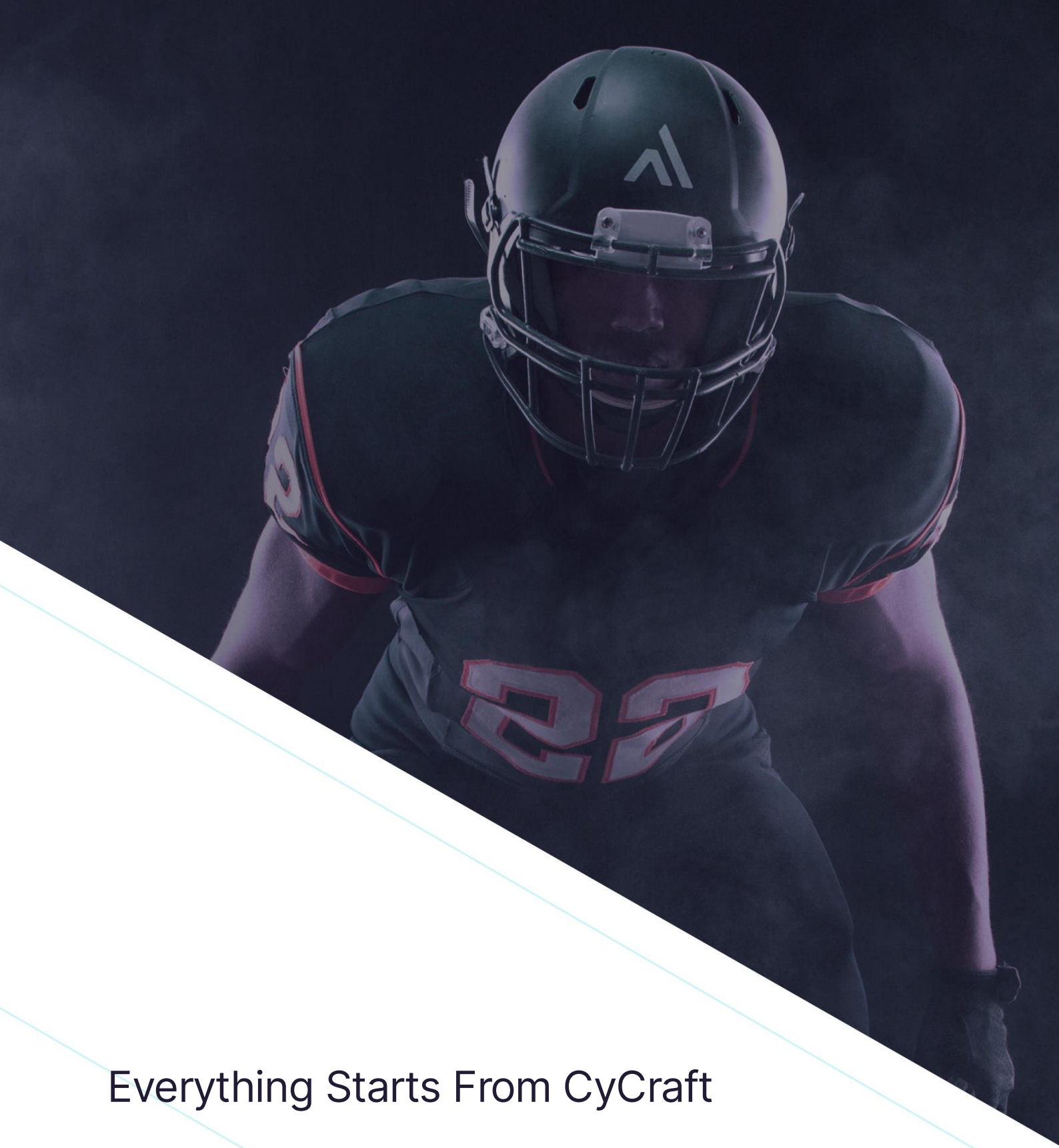
2022 年中國國家級駭客 APT 10 針對台灣金融業供應鏈攻擊 IOC 清單

CYCRAFT



Everything Starts From CyCraft

CyCraft is on AI company that forges the future of cybersecurity resilience through autonomous systems and human-AI collaboration.

入侵威脅偵測指標(IoCs)

Name	IOC	相關說明
Log.aspx	D42BF66485218F2ED76A8B1D63AF417FD2A82C8B	WebShell
PresentationCache.exe	4ECFC1A89B50CD8DC1B9424C3EFCF63E257525AA	DotNet Downloader
PresentationCache.exe	6E6C399BDA3C1F06ADE71053FDDD8FBEFA15029C	DotNet Downloader
PresentationCache.exe	EC30990EFD04B15926F2F9DB59F3BFDFEC413C23	DotNet Downloader
PresentationFrom.dll	7D8EDEDB3104FEE9A422FC4E97B1969DC31C4E66	DotNet Library
PresentationFrom.dll	CE2925BCD3188D3CB6F8BB67CD9D3F2D72FDDC05	DotNet Library
PresentationFrom.dll	BD6069BE81C70E918CF95BBDB30765A90A07FD98	DotNet Library
PresentationStatic.dll	333D9A94DC1A95D3C773BDE232D1BC2756C10518	DotNet Library
PresentationStatic.dll	6B47C2DEE1788017043B456C27E22193537B7A26	DotNet Library
PresentationStatic.dll	49E803BEAA4230E69A216B91757E35840D0C8683	DotNet Library
PresentationCheck.bin	A9541DEB16FFB41B6B4744D409597F9C62F7110E	DogCheck
PresentationCheck.bin	B6626AE6ED2F24FB82E262A2B766F2E5FD7E5230	DogCheck
x86.bin	7CB09DC4BC7DD68D6AACE7A9628634248F18EBA5	Quasar RAT

File Server	dowon[.]microsofts[.]top	香港 IP
File Server	dowon[.]08mma[.]com	resolve to 43[.]245[.]196[.]120 香港 IP
C2 Server	cahe[.]microsofts[.]org	香港 IP
C2 Server	cache[.]microsofts[.]cc	resolve to 104[.]155[.]228[.]182 桃園 IP
C2 Server	cahe[.]3mmlq[.]com	resolve to 43[.]245[.]196[.]121 香港 IP
C2 Server	cahe[.]7cnbo[.]com	resolve to 43[.]245[.]196[.]122 香港 IP
C2 Server	43[.]245[.]196[.]120	香港 IP
C2 Server	43[.]245[.]196[.]121	香港 IP
C2 Server	43[.]245[.]196[.]122	香港 IP
C2 Server	43[.]245[.]196[.]123	香港 IP
C2 Server	43[.]245[.]196[.]124	香港 IP
C2 Server	23[.]224[.]75[.]93	香港 IP
C2 Server	23[.]224[.]75[.]91	香港 IP


CYCRAFT
奧義智慧科技