Phase	January	February	March	April	May	June
Reconnaissance	Scan for email servers, find account credentials	Find users or systems that have access to CPS				
Weaponisation		Customise malware for CPS information gathering		Customise malware for RTU reset		
Delivery			Deploy malware to CPS through engineer’s USB thumb-drive		Deploy malware to CPS through engineer’s USB thumb-drive	
Exploitation	Access Virtual Private Network (VPN) connected to IT network	Compromise CPS engineer’s computer			Suppress alarm reporting to main server	Scheduled task executes and manipulates connected RTUs
Installation	Install Cobalt Strike beacon agent in IT network for remote access	Install Cobalt Strike beacon agent in private IT network connected to CPS	Malware executes and collects network information		Malware executes on CPS and hides its process, awaits scheduled task execution	
Command and Control (C2)	Establish remote connection with beacon in IT network	Establish C2 callback to beacon in IT network	Maintain C2 access	Malware detects engineer’s USB thumb-drive and saves CPS information in USB thumb-drive	Maintain C2 access	Maintain C2 access
Actions on Objectives	Establish initial (primary) foothold	Compromise ”patient zero”	Establish secondary foothold in CPS	Information harvesting and retrieval	Staging and preparation for final attack	CPS operations and services disrupted