Timestamp (UTC)	Motivation / Goal	Host	User	Description
13:32:36.520 - 13:32:36.533 (4 times)	Initial comprise	sql01 / epj01 / ad01 / ad02	SYSTEM	Cmd.exe spawned by svchost.exe across multiple systems, indicating an attempt to execute commands or scripts in a stealthy manner
13:35:12.086 - 13:36:12.131 (9 times)	Clear potential tracks	exchange01	-	Attempted or successful clearing of windows and event log data
15:40:36.619, 15:45:45.881 (2 times)	Initial comprise	confluence01	confluence, root	Potential shadow file read via command line utilities
15:42:54.655	Initial comprise	confluence01	confluence	Suspicious system commands executed by previously unknown executable
15:44:00.670 - 15:44:00.729 (17 times)	Initial comprise	confluence01	confluence	Suspicious Java child process executions on confluence01, suggesting exploitation of Java-based vulnerabilities or malicious Java applications
15:47:15.538 - 15:48:48.718 (4 times)	Clear potential tracks	exchange01	-	Attempted or successful clearing of windows and event log data
15:49:03.744 - 15:49:03.791 (4 times)	Initial comprise	confluence01	confluence	Suspicious Java child process executions on confluence01, suggesting exploitation of Java-based vulnerabilities or malicious Java applications
15:52:18.575 - 16:04:03.728 (8 times)	Clear potential tracks	exchange01	-	Attempted or successful clearing of windows and event log data
16:05:21.739	Malware Deployment	exchange01	confluence_sync	PlugX, a well-known remote access trojan (RAT), has been installed
16:07:27.645 - 16:09:06:724 (4 times)	Clear potential tracks	exchange01	-	Attempted or successful clearing of windows and event log data
16:15:27.810, 16:15:27.810 (2 times)	Malware Deployment	ad02	SYSTEM, confluence_sync	Unknown malware (pirpi.exe) has been installed
16:16:15.660 - 16:16:33.627 (3 times)	Lateral movement	ad02	confluence_sync, -	Initiation of remote file creation on a sensitive directory, then potential lateral tool transfer via SMB share
16:18:45.682	Persistence and privilege escalation	ad02	confluence_sync	User added to privileged group in active directory
16:19:42.810	Discover data	ad02	confluence_sync	WhoAmI-Discovery operation to obtain user insights
16:19:51.645, 16:19:51.650 (2 times)	Lateral movement	ad02	confluence_sync, -	Remote Execution via file shares
16:20:15.559, 16:20:15.562 (2 times)	Persistence and privilege escalation	ad02	confluence_sync	User account is created to ensur continued access to system
16:20:30:881 - 16:20:30:890 (3 times)	Malware Deployment	ad02	confluence_sync	Malware mimikatz.exe and text.exe is installed in ad02
16:20:36.744	Discover data	ad02	confluence_sync	Unusual discovery signal with unusual process command line detected
16:20:39.648	Persistence and privilege escalation	ad02	confluence_sync	User added to privileged group in active directory
16:22:36.705	Clear potential tracks	ad02	confluence_sync	Attempted or successful clearing of windows and event log data
16:23:33.714	Persistence and privilege escalation	ad01	SYSTEM	Exploitation of privilege escalation, first time driver is detected
16:24:21.751	Clear potential tracks	ad02	confluence_sync	Attempted or successful clearing of windows and event log data
16:25:33.850	Malware Deployment	ad02	SYSTEM	Malware text.exe is installed in ad02
16:25:42.773	Discover data	ad02	confluence_sync	Unusual discovery signal with unusual process command line detected
16:27:12.792 - 16:27:12.819 (14 times)	Persistence and privilege escalation	ad01, ad02	svc_exchange	COM Hijacking to ensure persistence, potential modification of registry
16:27:21.844 - 16:27:21.851 (4 times)	Clear potential tracks	ad02	SYSTEM, svc_exchange	Masquerading - Detection of a process execution from an unusual dirctory
16:30:39.753	Lateral movement	ad02	svc_exchange	Utilizing PsExec Network Connection for lateral tool transfer and lateral movement
16:30:39.786, 16:30:39.790 (2 times)	Malware Deployment	ad02	svc_exchange	Malware text.exe and doc.exe are installed in ad02
16:31:24.773 - 16:31:42.817 (5 times)	Lateral movement	ad01	svc_exchange, -	Initiation of remote file creation on a sensitive directory, then potential lateral tool transfer via SMB share
16:32:06.705	Persistence and privilege escalation	ad01	svc_exchange	Configuration event in which windows service was installed via an unusual client
16:34:01.051	Persistence and privilege escalation	ad01	svc_exchange	User added to privileged group in active directory
16:34:12.740, 16:34:12.740 (2 times)	Persistence and privilege escalation	ad01	svc_exchange, -	Installation of suspicious service in system has been detected
16:35:03.643, 16:35:03.643 (2 times)	Lateral movement	ad01	svc_exchange, -	Remote Execution via file shares
16:35:27.667, 16:35:27.670 (2 times)	Persistence and privilege escalation	ad01	svc_exchange	User account is created to ensur continued access to system
16:35:42.880 - 16:35:42.889 (3 times)	Malware Deployment	ad01	SYSTEM, svc_exchange	Malware doc.exe is installed or executed in ad01
16:35:45.712	Lateral movement	ad02	svc_exchange	Utilizing PsExec Network Connection for lateral tool transfer and lateral movement
16:35:48.754	Discover data	ad01	svc_exchange	Unusual discovery signal with unusual process command line detected
16:35:51.937	Persistence and privilege escalation	ad01	svc_exchange	User added to privileged group in active directory
16:37:24.619	Persistence and privilege escalation	ad02	EXCHANGE01$	Account configured with never-expiring password
16:43:12.586, 16:44:42.804 (2 times)	Clear potential tracks	ad02	confluence_sync	Attempted or successful clearing of windows and event log data
16:45:54.785	Persistence and privilege escalation	ad01	svc_exchange	Mimikatz.exe is executed to access the LSASS Process via the Windows API
16:45:54:858, 16:45:54:863 (2 times)	Malware Deployment	ad01	svc_exchange	Mimikatz.exe is detected, probably as a result of the previous execution
16:47:51.842, 16:47:51.842 (2 times)	Clear potential tracks	ad01	svc_exchange	Masquerading - Detection of a process execution from an unusual dirctory
17:21:22.229	Persistence and privilege escalation	ad01	svc_exchange	Mimikatz.exe is executed to access the LSASS Process via the Windows API
17:21:25.280	Malware Deployment	ad01	svc_exchange	Mimikatz.exe is detected, probably as a result of the previous execution
17:23:10.413 - 17:33:16.411 (4 times)	Clear potential tracks	ad01	SYSTEM, svc_exchange	Masquerading - Detection of a process execution from an unusual dirctory
17:36:34.339 - 17:36:34.348 (3 times)	Malware Deployment	ad01	SYSTEM, Tsvendsen_admin	doc.exe is detected
17:40:19.299	Clear potential tracks	ad01	Tsvendsen_admin	Attempted or successful clearing of windows and event log data
17:41:40.396	Malware Deployment	epj01	Tsvendsen_admin	doc.exe is detected on database server
17:43:31.340 - 17:46:43.212 (13 times)	Persistence and privilege escalation	epj01, ad01	Tsvendsen_admin	COM Hijacking to ensure persistence, potential modification of registry, as well as other persistence techniques
17:46:46.439, 17:46:46.446 (2 times)	Malware Deployment	epj01	Tsvendsen_admin	doc.exe and docss.exe are detected on database server
17:46:49.365	Discover data	epj01	Tsvendsen_admin	Unusual discovery signal with unusual process command line detected
17:49:40.397, 17:51:13.353 (2 times)	File Extraction	epj01	Tsvendsen_admin	Roshal Archive (RAR) or PowerShell File Downloaded from the internet, remote file download via powershell, preparation of data extraction
17:50:31.309	Clear potential tracks	epj01	Tsvendsen_admin	Attempted or successful clearing of windows and event log data
17:51:52.406, 17:51:52.411 (2 times)	Malware Deployment	sql01	Tsvendsen_admin	doc.exe is detected on database server sql01
17:53:37.402 - 17:53:37.413 (7 times)	Persistence and privilege escalation	sql01	Tsvendsen_admin	COM Hijacking to ensure persistence, potential modification of registry
17:54:13.307	Clear potential tracks	sql01	Tsvendsen_admin	Attempted or successful clearing of windows and event log data
17:55:13.427 - 17:56:52.290 (3 times)	Persistence and privilege escalation	sql01	Tsvendsen_admin	User added to privileged group in active directory, as well as "Boot or Logon Autostart Execution"
17:56:19.317	File Extraction	sql01	Tsvendsen_admin	Remote file download via powershell