

■ 侵入の痕跡 (Indicators of Compromise、IoC)

File/Path	SHA256	Detections
/<Install Path for WS02 Product>/repository/deployment/server/webapps/authentication endpoint/{6 Random letters}.jsp	2effebac6dc4fe8924315403f3dbda2fddfd7ea616faaf5cac2d7f6c85254e9e	Backdoor.Java.WEBSHELL.SMC
/<Install Path for WS02 Product>/repository/deployment/server/webapps/authentication endpoint/temp.jsp	d2ec9ec31013320eb3f4e1886a0e1a4720919761bd0cb62dbd66a9b8f13cc23d	
/<Install Path for WS02 Product>/repository/deployment/server/webapps/authentication endpoint/unit.jsp	9afec5620d7cfd959b3ec81442fefc05b4d0200194bc4443de7ea0b9f452b0f	
/<Install Path for WS02 Product>/repository/deployment/server/webapps/authentication endpoint/wso2is-08-22-2019_19_29.jsp	293eca7343c5cab11427431c93f66f972ce14061691ceb9bd7546b9fb283b1d0	Backdoor.Java.WEBSHELL.YXCDVZ
/<Install Path for WS02 Product>/repository/deployment/server/webapps/authentication endpoint/9.jsp	5c0970c2c253c2120d722c37aa397b1ce5fa61108f8441a84001eed5b565dc78	Backdoor.Java.WEBSHELL.YXCD4Z
<Install Path for WS02 Product>/repository/deployment/server/webapps/{5 letters like HcTnA}.war	<Hash values are shuffled for each sample>	JAVA_EXPLOIT.SBGX Trojan.Java.CVE20124681.D
<Install Path for WS02 Product>/repository/deployment/server/webapps/{5 letters like HcTnA}/WEB-INF/classes/metasploit/Payload.class	0c4c5c036272eb19d5617c9ce072e14ffb795a354dc682e6b0d144143ac4c7b4	Trojan.Java.CVE20124681.D

<Install Path for WSO2 Product>/tmp/LBcgqCymZQhm	4993806d2f77096ab28d589f8ee91869fc6045725ec9bc83b9e57f78cf86a5b8	Backdoor.Linux.COBEOCON.AA
<Install Path for WSO2 Product>/tmp/uCQeONYQ	58c0dd936dd314637a7a85db5227ed0ebbf33508372a646c09c98ec2dd4e5d	Backdoor.Linux.COBEOCON.AB
B0300521ED21DD328FA3A989E8229423	92443dfd40df1dc87976fc827e46a264979d5ed2a8e2153864d6f2725a9aab0c	Backdoor.Win64.COBEOCON.SMA
C:¥Windows¥Temp¥fscan.exe	d26437cc6ff9d094d42947d214c80a313e064ca403e9dd33a8110d7e859dd10e	HackTool.Win64.NetScan.AE
/dev/shm/hezb	aaa4aaa14e351350fccbda72d442995a65bd1bb8281d97d1153401e31365a3e9	Coinminer.Linux.MALXMR.SMDSL64
auto.sh	a3f08adadb93ee760f81ef96cc08810070f4f5a75d5417191975da5ab778766c	Trojan.SH.MALXMR.UWELO
setup_c3pool_miner.sh	0bade474b812222dbb9114125465f9dd558e6368f155a6cd20ca352ddd20549e	Coinminer.SH.MALXMR.YXBLU

URLs

- hxxp://13[.]94[.]40[.]162:8088/auto[.]sh
- 179[.]60[.]150[.]29:4444