Appendix 1 – IOCs and Yara rules for Ivanti Connect Secure ("ICS") VPN appliances

Code Family	Filename	Description
DRYHOOK	n/a	Credential Theft Tool
PHASEJAM	/tmp/s	Web Shell dropper
PHASEJAM Webshell	/home/webserver/htdocs/dana-na/auth/getComponent.cgi	Web Shell
PHASEJAM Webshell	/home/webserver/htdocs/dana-na/auth/restAuth.cgi	Web Shell
SPAWNSNAIL	/root/home/lib/libsshd.so	SSH backdoor
SPAWNMOLE	/root/home/lib/libsocks5.so	Tunneler
SPAWNANT	/root/lib/libupgrade.so	Installer
SPAWNSLOTH	/tmp/.liblogblock.so	Log tampering utility

Table 1 – IOCs (Source: Mandiant)