侵入の痕跡（IoC: Indicators Of Compromise）

SHA256	ファイル	検出名
ecdc8fade561a75d68235859ad8b1fe131db2c458b4894268e38e90ecab1c47f	st.txt	Backdoor.PS1.BANANARAT.A
38dfeb772afbd01c04eddda120d283acfb1147a6dc3d54ac62fe23ad06e39d8f	st.php	Trojan.PS1.BANANARAT.A
4912b1134e69ade7266e8508eec33ccb2d80ad693f1dbc4f1f4344c6dfcf2ff1	payload.php	Trojan.PS1.BANANARAT.A
d7545b6dacebdae27effb3c778c5e349027ec789c76ae4f777bd9ba56a70cdaa	msedge.txt	Backdoor.PS1.BANANARAT.A

IPアドレス / ドメイン	カテゴリ
hxxp[://]24[.]199[.]90[.]58:80/	Disease vector
hxxp[://]24[.]199[.]90[.]58:80/payload[.]php	Disease vector
hxxp[://]24[.]199[.]90[.]58:80/st[.]txt	Disease vector
c[.]windowsk-cdn[.]com	C&C server
162.141.111[.]227:443	C&C server