SEQRITE

IOCs

Archive File	
0725318b4f5c312eeaf5ec9795a7e919	Missile-Clean-room.zip
LNK	
ab11b91f97d7672da1c5b42c9ecc6d2e	Missile Clean room.pptx.lnk
HTAs	
cbaa7fc86e4f1a30a155f60323fdb72a	pantomime.hta
036da574b5967c71951f4e14d000398c	jquery.hta
DLLs	
5B9EAECCB041CB9C49CE78491CC5E965	hta.dll
CB9622956D074F7F5E0A1CAB37C9FF33	preBotHta.dll
2e19b7a2bbdc8082024d259e27e86911	DUser.dll
BAT	
05f9ac07249121d89cd4416ef466671c	test.bat
Domain	
cornerstonebeverly[.]org	
IPs	
160.153.131[.]201:443	Hosted HTA files
144.91.72[.]17:8080	C2
URLs	
hxxps://www.cornerstonebeverly[.]org/js/files/docufentososo/doecumentosoneso/pantomime.hta	
hxxps://www.cornerstonebeverly[.]org/js/files/Missile-Clean-room	
hxxps://cornerstonebeverly[.]org/js/files/ntfonts/avena/	
hxxps://cornerstonebeverly[.]org/js/files/ntfonts/winsteros.txt	
PDBs	
E:\Packers\CyberLink\Latest Source\Multithread Protocol Architecture\HTTP Arsanel\Clinet\app\Release\app.pdb	
E:\Packers\CyberLink\Latest Source\Multithread Protocol Architecture\HTTP Arsanel\Arsanel preBot\preBot\preBotHta\obj\Release\preBotHta.pdb	
EXE (Legitimate)	
9B726550E4C82BBEB045150E75FEE720	cridviz.exe