IOC	Description	Source	Hash
Svhost.exe	Remote Access Trojan (RAT) - SystemBC	CORPDC001	SHA256: f87f12c96f2dcf1b3feeff1fbb48a18a7717c500980829159f4d444677f29908
DESKTOP-3ITPFTA	Attacker workstation name	CORPDC001	
Qwe.exe	File	BOSDCSVR02	SHA1: bfd345a76b0a9f9d10200bb2d2579d08cf863a67
FH62SOSIWXSI.exe	Renamed PSEXEC	BOSDCSVR02	SHA256: 1409e010675bf4a40db0a845b60db3aae5b302834e80adeec884aebc55eccbf7
JM4wgY.exe	Play Encryptor	BOSDCSVR02	SHA1: a6efb02a138c2ec4a1c2debd8affebe47bb74543
GnwbE1.exe	Play Encryptor	BOSDCSVR02	SHA1: a6efb02a138c2ec4a1c2debd8affebe47bb74543
DX2QC4NKK3GC.exe	Renamed PSEXEC	BOSDCSVR02	SHA256: 1409e010675bf4a40db0a845b60db3aae5b302834e80adeec884aebc55eccbf7
144.202.81.117	Svhost.exe IP Comms - VirusTotal		
192.229.211.108	Svhost.exe IP Comms - VirusTotal		

Xxx.exe	Play Encryptor		SHA256: 633ad7ec10ca31b880be3be925077c392813ce2e6e7aef851a620b11515a2ad7
Svhost.sa	File	CORPDC003	SHA256: 236ce50caad844413fbecb3d19b2534c48155dd17e7f2fb4112bacaee3d6de73
209.127.184.163	Malicious download string - powershell	CORMGMTSVR004	
hxxp://209.127.184 .163:80/afdefb	Malicious download string - powershell	CORMGMTSVR004	
1.exe	S1 Detection		SHA1: a6efb02a138c2ec4a1c2debd8affebe47bb74543
0bxduo.exe	File	TESTAPPSVR020	SHA256: 633AD7EC10CA31B880BE3BE925077C392813CE2E6E7AEF851A620B11515A2AD7
D7Gbga.exe	File	TESTAPPSVR020	SHA256: 633AD7EC10CA31B880BE3BE925077C392813CE2E6E7AEF851A620B11515A2AD7
CBREQWSCEW2H	Malicious service around time of ransomware execution	CORPBLDSVR002	

WU8Q64NRPLJK	Malicious service around time of ransomware execution	CORPBLDSVR002	
Q9H3PX1PZQ8I.exe	File	TESTAPPSVR036	Not available from disk
FEKZXE3FVO8S.exe	File	TESTAPPSVR036	Not available from disk
Q9H3PX1PZQ8I	Malicious service around time of ransomware execution	TESTAPPSVR036	
FEKZXE3FVO8S	Malicious service around time of ransomware execution	TESTAPPSVR036	
PSEXEC-BOSDCSVR02-9248BFFA.key	PSExec usage	BOSDCSVR02	