

CERT

VoidCrypt r

2020 4 Case_ID

IEP

VoidCrypt

VoidCrypt

cmd.exe SQLWriter VoidCrypt AES+RSA

SQLBrowser MSSQLSERVER

MSSQL$CONTOSO1 MSDTC

SQLSERVERAGENT vds

VoidCrypt

Decryption-Info.HTA

2)

3)

ATT&CK

ATT&CK

1)

web

ATT&CK

2020 8 3 (241)
ntiynews@antiy.cn

标题	Four
	Phil S
	https://