

FTP MountLocker ChaCha20+
RSA RSA-2048

.ReadManual.

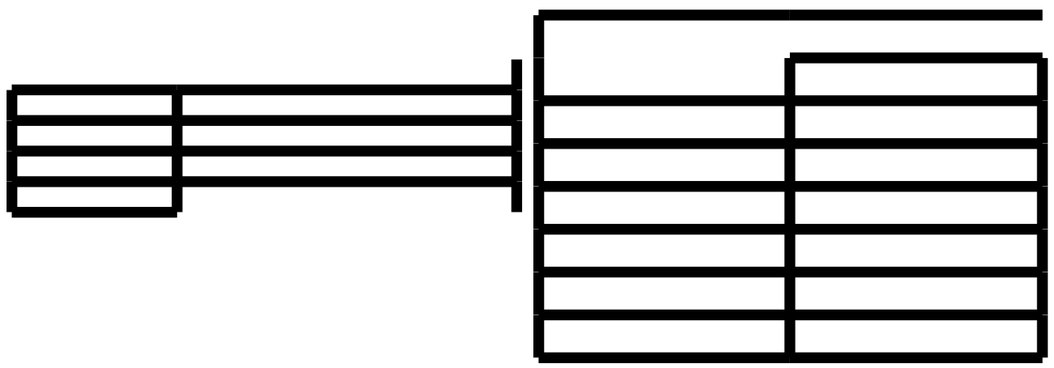
CERT
MountLocker RecoveryManual.html
2020 7
2020 11

CobaltStrike Beacon

VPN

IEP
MountLocker وسلم وسلم

MountLocker



MoleCloud

CERT 2020 10

ATT&CK

ATT&CK

ENIGMA ATT&CK
Spark 12 14
Moonlight .NET MoleStage
Molerats Gaza Hackers Team Gaza Python MoleCloud
Cybergang APT MoleCloud

2012 ClearSky 2016
Operation DustySky Web MoleCloud

11 30

Kawasaki Heavy
Industries

IT

.23/+640/7./6 - ./.+60671501

SolarWinds
SolarWinds hackers aimed at access to victims cloud assets
Pierluigi Paganini
365 Defender SolarWinds Sunburst/Solorigate SAML SAML SAML SAML
https://securityaffairs.co/wordpress/112773/hacking/solarwinds-solorigate-attack-chain.html