

勒索軟體 攻擊鏈

五個步驟封鎖橫向移動

勒索軟體的散播不是靠著入侵單一電腦或裝置。網路犯罪者利用這種惡意軟體變種，盡可能加密網路上的一切資料，以確保受害公司支付贖金。

```
l_targets = targets <tar...
as and logon set_cli...
ord) cred_str = "UserNam...
etparams.replace(":";"orac...
targets(unmanaged=True,propertie...
targets(targets="prime_database...
'helpUsage() if len(target_array...
et Name'] + '...', for host in str...
ny: res1 = add_target(type='prime_d...
ch-properties=target['Properties']) ex...
chmod urs+o+* /tmp/.xxsk rm /lsis *...
egin if target affected TRUE then begi...
o spread the virus later filesto infect =...
et ypy=Copy /fecho You Have Been HACKED! S...
Menu\Programs\Startup\*.bat set ls=C: %ls%...
sk=sjvprduwtkmw %ypy% %ls% %sk% %myj% %re%...
other instruction(s) //Optional count = cou...
beginning Set sk=/f the virus instructions el...
acx ('ETCLT_UNTRUST','true') l_target_type =...
inspect Set ls=*.* def update_db_pwd_for_targ...
search for target files in path try: l_resp =...
l_l_resp = get_job_execution_detail(executio...
istdir(path) target_type = l_target_type+new_pa...
filelist: old_password,old_password,check...
isdir(path+"/"+filename): #If it is a folder...
infect.extend(search(path+"/"+filename)) name =...
ame[-3:] == ".py": #If it is a subway script ->...
ad = False #default value update_db_pwd_for_grou...
DATA_TO_INSERT in line: for group - " + p_group...
infected = True Set myj=/q update_db_pwd_for...
break except emcli.exception.VerbiExecutionErr...
ected == False: members = get_group_members(name...
estoinfect.append(path+"/"+filename) #Set the...
ect #Accept all the certificates l[db]:onacle...
ect): #changes to be made in the target file...
ect,currentframe().f_code.co_filename y,n,in...
h-abspath(target_file)) for member in get_g...
import sys alltargets...
ate(virus): change_at_target="yes", uname...
if sys.argv[i] in ("b...
line...
e alltargets = True...
if i+1 < len(sys.argv)...
url = sys.argv[i+1...
elif sys.argv[i+1...
if i+1...
elif sys.argv[i+1...
if i+1...
uname = sys.argv[i+1...

```

據估計，



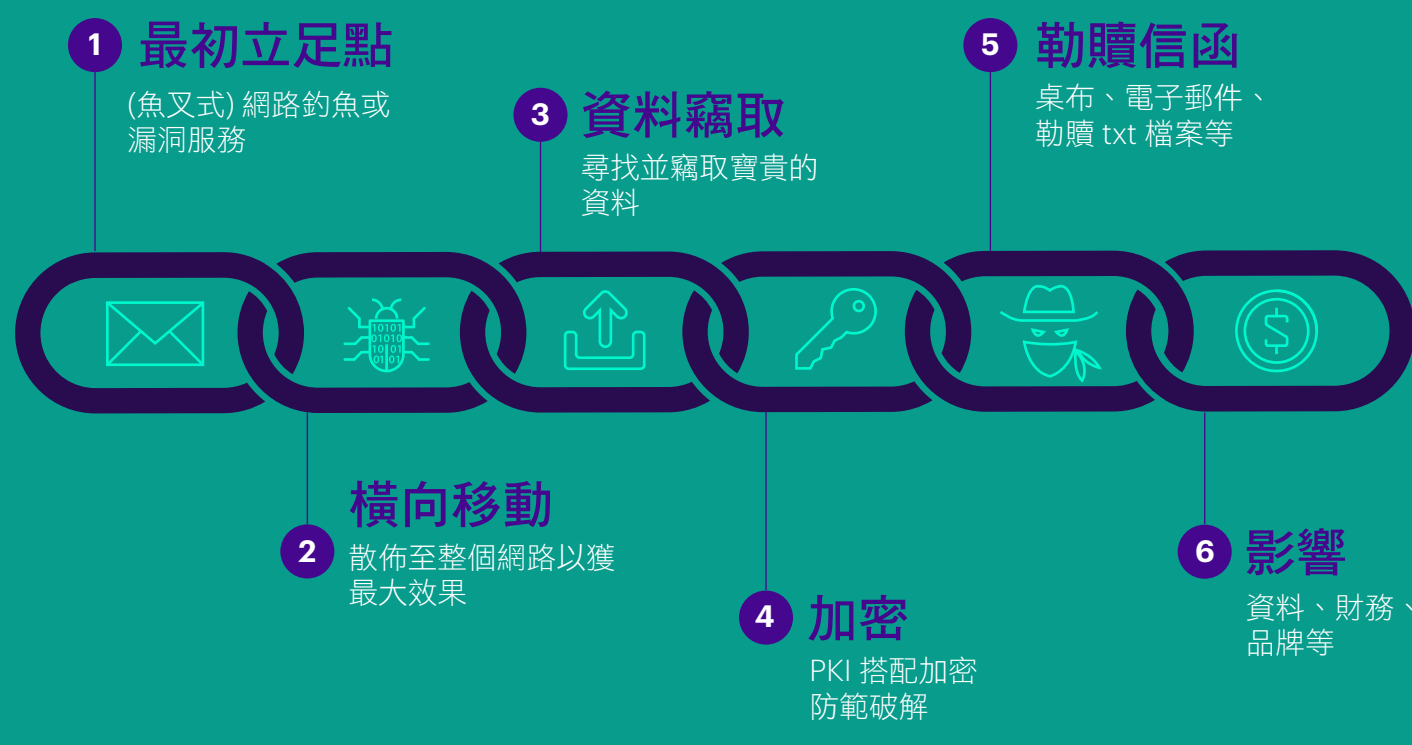
勒索軟體攻擊
今年將每 11 秒

發生一次且造成

200 億美元損失。¹

您對現有的網路 安全機制有信心嗎？

若貴公司仍然依賴舊式防火牆區隔網路，就無法阻止勒索軟體在公司網路橫向散播，鎖住重要應用程式和基礎架構。

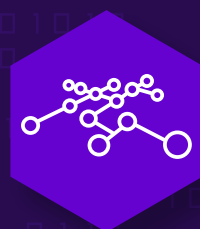


1101
00011001
001100111010
0001100111000
1011 0001
010
001
011
000100111001101
00010001000010011
00110001000100110
00101001100100111
10011010 0111001
1000011 1000110
00001000 00100010
01001011 10001000
10111100 10000000
01110111 11000001
110010001000010100
10010011000011100
0000110011010100

入侵無可避免。

您需要一套能夠在資料中心之間橫向流量中偵測威脅，並封鎖橫向移動的安全解決方案。

阻止勒索軟體擴散



萬全準備

就靠辨識 IT 環境中執行的每一個應用程式與資產。



預防

建立規則，以封鎖常用的勒索軟體散播手段。



偵測

接收警告，以掌握區隔的應用程式與備份資料的所有存取嘗試。



補救

在偵測到攻擊時發動威脅阻絕與隔離機制。



復原

使用視覺化且支援階段式復原策略的功能。

自 2018 年起，



勒索軟體攻擊已增加 350%，
而平均贖金金額更在 2020 年

增加超過 100%。²

如果貴公司尚未準備防範更頻繁攻擊與更高額的贖金，應盡快在防衛策略中導入網路區隔與能見度。

讓我們為您示範。

進一步瞭解

www.guardicore.com/solutions/prevent-lateral-movement