學術網路風險威脅評估報告-1

■ 說明

隨著網路的興起，相關的網路攻擊事件也層出不窮。為了因應此新興的威脅，教育部於 TANet 網路上部署了不同的偵測點來偵測相關的網路威脅並記錄於 SOC 資料庫中。因此 TACERT 與南區教育學術資訊安全監控中心 (South-Academic Security Operation Center，簡稱 S-ASOC)合作，分析其所記錄的威脅資訊，從中取得駭客所熱衷攻擊的網路服務資訊，並分析其所使用之攻擊手法及提出相對應之應變措施，除此之外，TACERT 運用”主動式網路威脅偵測系統”來偵測 TANet 內之主機是否正在運作相關的網路服務，而曝露在潛在的威脅之中。

■ S-ASOC 偵測資料分析

本份資料源自 S-ASOC 107 年度 1 至 4 月所偵測到的資訊，TACERT 從此份資料中，能夠取得在此期間，駭客所熱衷攻擊的網路服務類型及其所運用的攻擊手法，相關資訊如下表所示（次數）。

服務名稱/月份	**201801**	**201802**	**201803**	**201804**
RDP	1222111546	986049533	1224188179	1021918282
udp/53413	642780605	496573641	1860390725	961327538
TELNET	562549417	565945067	508142954	449283335

■ 攻擊手法說明

在本節中，TACERT 針對上述相關網路服務的攻擊手法進行說明

■ ＲＤＰ網路服務

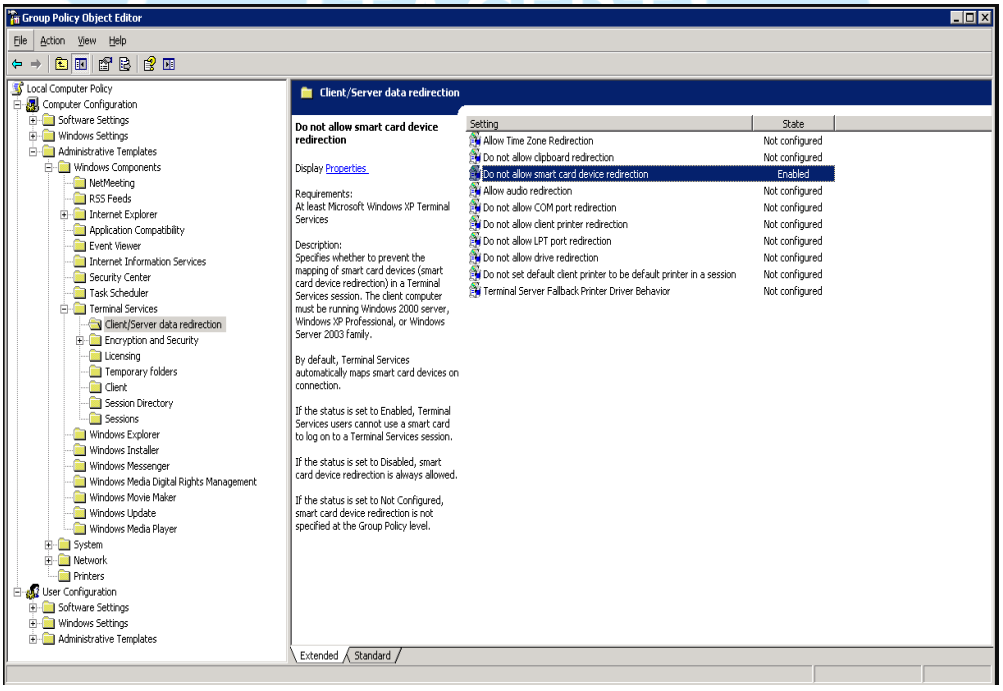
網路服務	RDP
威脅名稱	MS.RDP.Connection.Brute.Force
說明	RDP（Remote Desktop Protocol）為微軟所提供的遠端桌面服務，它允許使用者以帳號及密碼的方式從遠端登入，並提供類似桌面的方式來操作受控主機。此服務的通訊埠預設於埠 3389 上，也因其認證方式僅使用帳號及密碼來進行驗證。因此常遭受到外部攻

	擊者以暴力猜測密碼的方式來進行攻擊。 MS.RDP.Connection.Brute.Force 表示當某個單一的來源端在 10 秒內進行了超過 200 次的猜測遠端桌面服務的密碼,即判定該來源端正在進行 RDP 的暴力攻擊
影響產品	所有提供 RDP（Remote Desktop Protocol）桌面服務的產品
影響層面	當攻擊者成功的猜測出帳號及密碼時，即可取得系統上的該帳密所歸屬的使用者權限（例如猜測出 administrator 的使用者，即取得該使用者的權限）。因此攻擊者可利用此類的權限來更動系統上的檔案或安裝任意的軟體
修正說明	如果非必要，建議關閉此項服務。 如果確實需要開啟此項服務，建議利用防火牆來限制來源端，設定僅允許管理者的主機可登入。而不要對外完全開放

網路服務	RDP
名稱	MS.Windows.RDP.ESTEEMAUDIT.Code.Execution
說明	在 Windows 2000 之後版本的驗證機制新增了以智慧卡(SmartCard)方式驗證。此漏洞即發生在智慧卡驗證程式。而在 Windows XP 及 Windows 2003 的遠端桌面(RDP)服務即使用具有此漏洞的驗證程式。因此，在上述的作業系統中的 RDP 服務即可能具有此類的漏洞。要利用此漏洞相當的簡單，只要利用發送一個特製的驗證封包至具有此漏洞的 RDP 服務上，即可能觸發此漏洞，而在該主機上造成 RCE(remote code execution,遠端執行程式碼)，在系統上執行任意程式。值得注意的是此漏洞的攻擊碼已被"Shadow Broker"駭客組織以 ESTEEMAUDIT 的名稱廣為散佈。Shadow Broker 是 2016 年夏季出現的一個駭客組織，曾發布了針對企業防火牆及微軟相關軟體的漏洞攻擊程式，其中最著名的即為 EternalBlue 攻擊工具。此工具曾被應用在 WannaCry 蠕蟲攻擊
CVE	CVE-2017-0176，CVE-2017-9073
影響產品	Windows XP Windows XP SP1 Windows XP SP2 Windows XP SP3 Windows 2003 Windows 2003 SP1

	Windows 2003 SP2
影響層面	當攻擊者成功的攻擊後，即可取得該系統的系統權限，因此可輕易更動系統上的檔案或安裝任意的軟體。
修正說明	由於微軟目前已停止對於 Windows XP 及 Windows 2003 產品線的支援，因此並未針對此漏洞發佈相對應安全修正程式。 建議使用者能儘快停用相關作業系統，並使用其它更新的作業系統。如果因為現實的考量而必需使用上述的作業系統，建議停用智慧卡(Smart Card)的驗證方式。 在 Windows server 2003 及 Windows XP 系統下停用智慧卡驗證方式，執行如下列指令 <1>在命令列模式執行 gpedit.msc 指令 <2>至” Computer Configuration\Administrative T emplates\Windows Components\Terminal Services\Client/Server data redirection\”機碼下 <3>設定 "Do not allow Smart Card device redirection"機碼為 enable <4>重新啟動電腦

停止智慧卡機碼畫面如下



■ **udp/53413 網路服務**

網路服務	udp/53413
名稱	Netcore.Netis.Devices.Hardcoded.Password.Security.Bypass
說明	在 2014 年中國一款路由設備(品牌名稱為 Netcore 或 Netis) ，即被證明其所使用的韌體(firmware)存在後門程式。此韌體將預設密碼以硬編碼(Hard Code)的方式寫入韌體內。並以服務(service)的方式，在通訊埠 53413 進行後門程式的運作，遠端攻擊者可藉由連接 53413 埠的方式，即可以預設密碼登入至該路由設備中，在該路由設備執行任意命令以及上傳、下載檔案及得到網頁登入的帳號及密碼等資訊。
影響產品	所有 Netcore/Netis 路由器
影響層面	使用者可完全的控制此設備
修正說明	建議根據 Netcore/Netis 路由器使用手冊的說明，重新更新韌體。並調整防火牆規則限制外部連線至通訊埠 53413

■ **Telnet 網路服務**

網路服務	Telnet
名稱	Telnet.Login.Brute.Force
說明	Telnet.Login.Brute.Force 是對於 Telnet 服務進行進行帳號及密碼的猜測(即暴力攻擊法)。 Telnet 是一種古老的傳輸協定，可允許使用者遠端連線至 Telnet 伺服器進行操作，但由於其認證所使用的帳號及密碼皆以明碼的型式進行傳輸而可能造成安全性上的漏洞，因此逐漸被其它的傳輸協定（例如:SSH）所取代。但近年來，由於物聯網(IoT)的盛行，許多的相關設備(例如:ipcam)即會採用 Telnet 的傳輸協定來進行遠端的連線，甚至有些設備會內建預設帳號及密碼,這也造成 Telnet 的暴力攻擊法越發猖獗。 Telnet.Login.Brute.Force 表示當某個來源端在一分鐘內登入失敗超過 60 次即表示其正在進行 Telnet 的暴力攻擊法。
影響產品	所有開啟 telnet 服務的產品

影響層面	使用者可完全的控制此設備
修正說明	如果非必要，建議關閉 telnet 服務。並建議查閱使用手冊的說明，確認已更改或關閉預設帳號及密碼。 在開啟 telnet 服務下，建議調整防火牆設備，限制可連線的來源端範圍。

網路服務	Telnet
名稱	Zivif.PR115-204-P-RS.Web.Cameras.Hardcoded.Password
說明	在市面上有某些網路監視器(IP Camera)產品在出廠時即會內建預設帳號及密碼，並提供 telnet 服務讓使用者登入使用。而使用者在使用此類產品時，常常也會因為疏忽而忘記更改此預設密碼， 也因此遠端攻擊者常會利用以預設帳號密碼登入的方式來嘗試登入至被攻擊目標 telnet 服務中，一但登入成功即能完全的控制該台設備。而 Zivif.PR115-204-P-RS.Web.Cameras.Hardcoded.Password 即表示遠端攻擊者正嘗試利用 Zivif 產品的預設帳號及密碼進行攻擊。 除此之外，如下資訊為已廣為流傳的網路監視器的預設帳號及密碼 ＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝ Acta: admin / 123456 Appro: admin / 9999 Avigilon: admin / admin Axis: root / pass Basler: admin / admin Boschs: service / service Brickcom: admin / admin Canon: root / (Camera Model) CBC: admin / admin CNB: root / admin Dahua:admin / admin ,888888/888888,666666/666666 Dynacol: admin / 1234 GeoVision: admin / admin Grandstream: admin / admin GVI: admin / 1234

	Hikvision: admin / 12345 Honeywell: administrator / 1234 IOImag: admin / admin IPX-DDK: root / admin IQinVisions: root / system JVC: admin / JVC Merit Lilin: admin / pass Messo: admin / (Camera Model) Mobotixs: admin / Meins , admin / meinsm Panasonic: admin / 12345 Pelco Sarix: admin / admin Pixord: admin / admin Riva-Rivatech: root / pass QViS: admin / 1234 Samsung Electronics: root / root , admin / 4321 Samsung Techwin (new): admin / 4321 Samsung Techwin (old): admin / 1111111 Sanyo: admin / admin Scallop: admin / password Sony: admin / admin Stardot: admin / admin Toshiba: root / ikwd Trendnet: admin / admin Telexper / txper: admin / 99999999 Ubiquiti: ubnt / ubnt UNV (Uniview): admin / 123456 Verint: admin / admin VideoIQ: supervisor / supervisor Vivotek: root / 空
CVE	CVE-2017-17107 CVE-2018-5723
影響產品	Zivif PR115-204-P-RS V2.3.4.2103 之前的版本 MASTER IPCAMERA01 3.3.4.2103 之前的版本
影響層面	使用者可完全的控制此設備
修正說明	如果非必要，建議關閉 telnet 服務。並建議查閱使用手冊的說明，確認已更改或關閉預設帳號及密碼

	在開啟 telnet 服務下，建議調整防火牆設備，限制可連線的來源端範圍

網路服務	Telnet
名稱	ZyXEL.PK5001Z.Modem.Backdoor
說明	在某些舊型的合勤(ZyXEL，https://www.zyxel.com/)的路由器，提供了 telnet 服務供管理者連線至設備上進行管理。但在某些機型上（目前確認的機型為 ZyXEL PK5001Z，其它的機型可能也具有相同的問題）預設了 root(超級用戶)的密碼為 zyad5001 及一般使用者的帳號/密碼(admin/CenturyL1nk)，惡意的攻擊者可先利用一般使用者權限登入至 telnet 服務後再以 su 指令轉換成 root 用戶，即可取得該系統上的超級使用者（root）的權限，進而控制整台路由器。
CVE	CVE-2016-10401
影響產品	ZyXEL PK5001Z Modem
影響層面	使用者可完全的控制此設備
修正說明	如果非必要，建議關閉 telnet 服務。並建議查閱使用手冊的說明，確認已更改或關閉預設帳號及密碼。 在開啟 telnet 服務下，建議調整防火牆設備，限制可連線的來源端範圍。

■ TANet 潛在風險

為遵循教育部之資安規定，對於 TANet 內之主機偵測通訊埠範圍將只限於 3389, 23,9100, 445, 53413，因此系統只針對上述通訊埠進行偵測。

掃描時間	2018-09-01 至 2018-09-30
掃描總數	135,872 台主機

➢ **具有潛在風險通訊埠資訊**

網路服務(通訊埠)	**總數**
telnet(23)	72
RDP(3389)	11

網路列表機(9100)	47
SMB (445)	0
通訊埠(53413)	0

■ 結論說明

RDP 服務由於其方便易用的特性，常被使用者用來遠端登入的管理用途上，也因此常成為惡意攻擊者覬覦的對像，也因此分析 SOC 所偵測的攻擊事件，RDP 的暴力攻擊常居於榜上前三名內，以 2018 年 1 月至 4 月的分析資料為例，RDP 攻擊更是位居首位。建議使用者如果一定需要開啟 RDP 服務，務必要利用資安設備來限制來源端的連線。

另一方面，由於近年來 IoT 設備（以下簡稱為設備）的興起，此類的攻擊也有日漸增多的趨勢，而綜合此類攻擊手法，均是利用設備的設定錯誤(例如：未更改設備之預設帳號及密碼）來進行攻擊。建議使用者在使用此類設備時，預必要先行詳閱設備之使用手冊。若發現有預設帳號密碼，務必進行修改。除此之外，此類設備常會啟動 telnet 服務來供使用者遠端連線之用，在一般的情況下，並不需要此類服務，強烈建議使用者關閉此類服務。