發佈編號	TACERT-ANA-2021061010063434	發佈時間	2021-06-10 10:09:35
事故類型	ANA-資安訊息	發現時間	2021-06-09 16:16:36
影響等級	低		

[主旨說明:]【資安訊息】日本 NISC 分享勒索軟體攻擊警示與防護建議，供各會員參考運用

[內容說明:]

轉發 國家資安資訊分享與分析中心 資安訊息警訊 NISAC-ANA-202106-0512

日本 NISC 近期分享勒索軟體攻擊與防護建議予其關鍵基礎設施營運商，技服中心綜整防護建議供各會員參考運用，詳見建議措施。

情資分享等級: WHITE(情資內容為可公開揭露之資訊)

[影響平台:]

1. 【預防】防止勒索軟體感染近期勒索軟體入侵途徑包含以下 5 種管道：
   (1) 經由網際網路直接攻擊連網設備之漏洞。
   (2) 利用特定通訊協定(RDP、SMB)或已知漏洞進行攻擊。
   (3) 因應疫情建構之遠距辦公環境資安防護不足。
   (4) 從海外據點等資安防護較弱的地點進行攻擊。
   (5) 透過其他惡意軟體進行感染。

因應前述勒索攻擊之可能途徑，建議採取以下防護措施：

(1) 檢視對外服務主機之安全性

應儘速進行安全性更新、管控外部管理主機之功能、僅開放必要服務並關閉不必要之通訊埠(如 137, 138, 139, 445, 3389 等)、落實 IT 資產管理。

針對 SMB 與 RDP 等通訊協定應採「原則禁止，例外開放」政策，啟用 SMB 時亦應禁用 SMBv1 協定，請重新檢視包括防火牆在內的對外服務主機均符合前述設定。

(2) 請關注以下已知被勒索軟體利用的軟體與設備漏洞，並及時進行修補：

- Fortinet VPN 設備漏洞 (CVE-2018-13379)
- Ivanti VPN 設備 Pulse Connect Secure 漏洞 (CVE-2021-22893、CVE-2020-8260、CVE-2020-8243、CVE-2019-11510)
- Citrix Application Delivery Controller、Citrix Gateway、Citrix SD-WAN WANOP 漏洞 (CVE-2019-19781)
- Microsoft Exchange Server 漏洞 (CVE-2021-26855 等)
- SonicWall SMA100 漏洞 (CVE-2021-20016)
- QNAP NAS 漏洞 (CVE-2021-28799、CVE-2020-36195、CVE-2020-2509 等)
- Windows Domain Controller 漏洞 (CVE-2020-1472 等)

(3) 針對遠距辦公攜出、長期休假等長時間未受到組織管控之電腦，在重新使用前應立即進行安全性修補、病毒掃描等防護措施。

(4) 近期發現 Emotet 惡意程式的後繼者 IcedID 惡意程式，會透過電子郵件進行攻擊，各防毒軟體已製作病毒碼，應及時進行防毒軟體更新、執行定期掃描、建立電子郵件防護機制等防護措施。

2. 【預防】降低資料加密造成之損害

備份雖為對抗勒索軟體之有效措施，惟駭客為增加取得贖金之機會，會先竊取機敏資料後再進行資料加密，若被駭者不繳付贖金，即公開機敏資料。面對前述雙重勒索之攻擊，應重新檢視與制定嚴格的機敏資料管理措施，相關防護措施如下：

(1) 確認定期備份機制與設定

確認即使在勒索軟體感染的情況下，備份資料也受到保護。例如採取 3-2-1 備份原則，將資料複製 3 份備份，保存在 2 種不同類型的儲存媒體，並將其中 1 份備份離線存放。

(2) 確認備份資料可有效還原。

(3) 針對機敏資料進行存取控制管控與資料加密。

(4) 確認組織已制定系統重建與資料還原計畫，並妥善施行。

3. 【偵測】及時偵測未授權之存取行為

組織應考設置專職之監控人員或透過自動化機制快速偵測未經授權之存取行為，防護措施如下：

(1) 加強對伺服器、網路設備及個人電腦等設備之日誌監控。

(2) 可利用端點偵測及回應機制(Endpoint Detection and Response, EDR)、持續診斷與緩解機制(Continuous Diagnostics and Mitigation, CDM)等加強偵測異常行為。

4. 【應變/復原】快速事件應變處理

組織應建立統一之事件應變處理機制，以利於遭受勒索軟體攻擊時，冷靜進行事件應變處理，防護措施如下：

(1) 確認組織已制定勒索軟體應變計畫，包含資料加密、資料外洩及阻斷服務等攻擊之應變處理與營運持續計畫。

(2) 確認組織員工發現勒索軟體感染跡象時，能及時聯繫系統管理人員。

(3) 確認組織內外部連繫管道與溝通機制，以便於遭勒索軟體攻擊時，可迅速連繫相關利害關係單位(包括承包商、相關組織及政府機關等)。

[參考資料:]

日本 NISC 情資原文：https://www.nisc.go.jp/active/infra/pdf/ransomware20210430.pdf