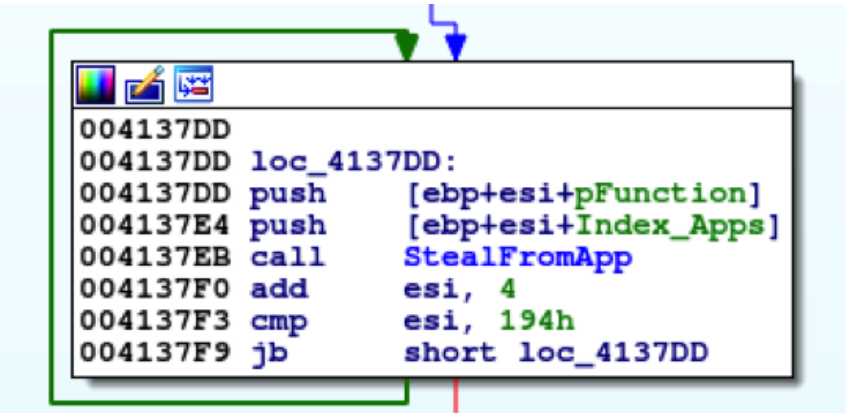
مرکز ماهر

آشنایی با بدافزار Dyzap

اصولا یکی از مبناهای اصلی طراحی بدافزار ها با هدف سرقت اطلاعات محرمانه از برنامه‌های کاربردی و سازمانی است و امرزه بدافزار های مدعددی با این رویکرد طراحی شده و دنیای سایبری را با مشکل مواجه میکنند. بدافزار Dyzap متعلق به این خانواده است و این کار را بوسیله‌ی عملیاتی نمودن یک حمله‌ی مرد میانی (به اختصار MITB) در مرورگرهای رایج انجام می‌دهد. بخش تحقیقات مرکز FortiGuard به تازگی گونه‌ی جدیدی از تروجان Dyzap را کشف کرده‌اند. اطلاعات به سرقت رفته می‌تواند شامل اطلاعات سیستمی و مدارک مربوط به برنامه‌ها که در سیستم آلوده ذخیره شده‌اند باشد، اما تنها به این موارد محدود نمی‌شود. در ادامه توضیح خواهیم داد که این بدافزار چگونه حساب‌های کاربری را به سرقت می‌برد و مانند یک کی‌لاگر (کلید دزد) عمل نموده و چگونه با سرور فرمان و کنترل (به اختصار C&C) خودش ارتباط برقرار می‌کند.

آشنایی با نحوه‌ی سرقت اطلاعات توسط بدافزار Dyzap

Dyzap برای عمل سرقت اطلاعات، بیش از یک‌صد برنامه را هدف قرار می‌دهد، از جمله مرورگرها، برنامه‌های پروتکل انتقال فایل (FTP)، و غیره.



شکل ۱. روال ساده عملیات سرقت.

به منظور سرقت اطلاعات از انواع مختلف برنامه‌ها، Dyzap برای هریک به روش مختلفی عمل می‌کند. این توانایی سرقت اطلاعات از پایگاه‌های داده، رجیستری‌ها، و همچنین از فایل‌های برنامه‌هایی که روی سیستم آلوده نصب شده‌اند را به بدافزار ذکر شده می‌دهد. تعدادی از برنامه‌های مورد هدف این بدافزار، مانند Fossamail، Postbox است که در شکل ۲ نشان داده شده است.

```
aSComodoIcedr_0:                        ; DATA XREF: sub_408C33+171↑o
                unicode 0, <%s\Comodo\IceDragon\Profiles\%s>,0
aSNetgateTechno:                        ; DATA XREF: sub_408C33+192↑o
                unicode 0, <%s\NETGATE Technologies\BlackHawk\profiles.ini>,0
                align 4
aSNetgateTech_0:                        ; DATA XREF: sub_408C33+1B6↑o
                unicode 0, <%s\NETGATE Technologies\BlackHawk\Profiles\%s>,0
aSPostboxProfil:                        ; DATA XREF: sub_408C33+1D3↑o
                unicode 0, <%s\Postbox\profiles.ini>,0
aSPostboxProf_0:                        ; DATA XREF: sub_408C33+1E3↑o
                unicode 0, <%s\Postbox\Profiles\%s>,0
                align 8
aS8pecxstudiosC:                        ; DATA XREF: sub_408C33+20D↑o
                unicode 0, <%s\8pecxstudios\Cyberfox\profiles.ini>,0
                align 8
aS8pecxstudio_0:                        ; DATA XREF: sub_408C33+21A↑o
                unicode 0, <%s\8pecxstudios\Cyberfox\Profiles\%s>,0
                align 8
aSMoonchildProd:                        ; DATA XREF: sub_408C33+23E↑o
                unicode 0, <%s\Moonchild Productions\Pale Moon\profiles.ini>,0
aSMoonchildPr_0:                        ; DATA XREF: sub_408C33+255↑o
                unicode 0, <%s\Moonchild Productions\Pale Moon\Profiles\%s>,0
                align 4
aSFossamailProf:                        ; DATA XREF: sub_408C33+27D↑o
                unicode 0, <%s\FossaMail\profiles.ini>,0
aSFossamailPr_0:                        ; DATA XREF: sub_408C33+290↑o
                unicode 0, <%s\FossaMail\Profiles\%s>,0
```

شکل ۲. بخشی از برنامه‌های مورد هدف بدافزار برای سرقت.

برای درک بهتر روش های مختلفی که Dyzap می‌تواند اعمال کند، چهار برنامه را انتخاب کرده‌ایم و نحوه‌ی دستیابی این بدافزار به اطلاعات ورود حساب آنها را بررسی کردیم. تحلیل‌هایی که در ادامه خواهند آمد، روی نسخه ۳۲بیتی ویندوز ۷ انجام شده‌اند. مسیرهای اشاره شده ممکن است در سیستم‌عامل‌های دیگر، متفاوت باشند.

خانواده‌ی Chrome.

یکی از روش‌های اصلی Dyzap، سرقت اطلاعات ورود حساب از فایل پایگاه داده‌ی sqlite3 است. بعنوان مثال، کرومیوم (پروژه‌ای برای ساخت مرورگر وب متن باز) اطلاعات ورود را در فایلی به اسم "Login Data" یا "Web Data" ذخیره می‌کند. این بدافزار با استفاده از قطعه کدها و مسیرهای فایل که بصورت کدسخت (کدی که بجای استفاده از متغیرها، داده‌ها ثابت قرار داده می‌شوند) نوشته شده‌اند، به دنبال مسیرهایی خواهد گشت که شامل فایل‌های ذکر شده باشند. اگر این فایل موجود باشد، بدافزار محتوای آن را داخل یک فایل موقت کپی می‌کند تا در عملیات بعدی مورد استفاده قرار دهد.

برای بدست آوردن اطلاعات ورود، ابتدا باید تایید کند که هدف یک فایل SQlite3 است. سپس یک الگوی رشته‌ای "منحصر به فرد" را جستجو می‌کند تا اطلاعات ورود را از جدول "logins" استخراج کند. در نهایت حساب کاربری را با استفاده از الگوهای رشته‌ای "password_value" ، "username_value" ، و "original_url" استخراج میکند.

```
push    offset aSSUserDataDe_0 ; "%s\\%s\\User Data\\Default\\Web Data"
call    AppendFormatedString
mov     esi, eax
add     esp, 10h
test    esi, esi
jz      short loc_407A48
push    esi
call    DoesFileExist
pop     ecx
test    eax, eax
jnz     short loc_407A48
push    esi             ; lpMem
call    HeapFree_0
push    [ebp+Subdirectory]
push    [ebp+Dirctory]
push    offset aSSLoginData ; "%s%s\\Login Data"
call    AppendFormatedString
mov     esi, eax
add     esp, 10h
test    esi, esi
jz      short loc_407A48
push    esi
call    DoesFileExist
pop     ecx
test    eax, eax
jnz     short loc_407A48
push    esi             ; lpMem
call    HeapFree_0
push    [ebp+Subdirectory]
push    [ebp+Dirctory]
push    offset aSSDefaultLogin ; "%s%s\\Default\\Login Data"
```

شکل ۳. جستجوی Dyzap برای فایل مربوطه در مسیرهای نوشته شده بصورت کدشکت.

```
00407F0A push    edi
00407F0B push    offset aPassword_value ; "password_value"
00407F10 push    offset aUsername_value ; "username_value"
00407F15 push    offset aOrigin_url ; "origin_url"
00407F1A push    3
00407F1C pop     ebx
00407F1D push    ebx
00407F1E push    offset aLogins  ; "logins"
00407F23 push    esi
00407F24 call    LookUpLoginData
00407F29 add     esp, 18h
00407F2C mov     edi, eax
00407F2E push    offset Add_UserName_Pass_URL_ToPacket
00407F33 push    offset VersionNumebr
00407F38 push    ebx
00407F39 test    edi, edi
00407F3B jz      short loc_407F58
```

شکل ۴. جستجوی Dyzap برای اطلاعات ورود، با استفاده از رشته‌های نوشته شده بصورت کدشکت.

برای دیگر مرورگرهای این خانواده، روالی بسیار مشابه تکرار می‌شود. از جمله مرورگرهایی که توسط این بدافزار بتازگی آلوده شده اند: Comodo Dragon ، MapleStudio ، Chrome ، Nichrome ، RockMelt ، Spark ، Chromium ، Titan Browser ، Torche ، Yandex ، Epic Privacy Browser ، CocCoc Browser ، Vivaldi ، Comodo Chromodo ، Superbird ، Coowon ، Mustang Browser ، 360Browser ، CatalinaGroup Citrio ، Chrome SxS ، Orbitum ، Iridium ، و Opera .

خانواده‌ی فایرفاکس.

در مورد مرورگرهای خانواده‌ی فایرفاکس، Dyzap فایلهای signons.sqlite و login.json را جستجو می‌کند تا مدارک مورد نظر را مکان‌یابی کند و به سرقت ببرد. فایل login.json با وجود اسم گمراه‌کننده‌ای که دارد، درواقع یک پایگاه داده‌ی sqlite است که شامل تمامی اسامی و رمزهای عبور حساب‌های کاربری‌ست. این خانواده از مرورگرها عبارتند از Firefox ، IceDragon ، Safari ، K-Melon ، SeaMonkey ، Flok ، Thunderbird ، BlackHawk ، Postbox ، Cyberfox ، و Pale Moon .

پروتکل انتقال داده‌ی Far.

بدافزار Dyzap علاوه بر سرقت فایل‌های پایگاه داده، تلاش می‌کند اطلاعات محرمانه‌ی برخی برنامه‌های پروتکل انتقال داده را از رجیستری به سرقت ببرد. برای نمونه در پروتکل انتقال داده‌ی Far، این بدافزار به راحتی مسیرهای زیر را جستجو می‌کند، که نحوه امر در شکل ۵ نشان داده شده است:

- HKCU\Software\Far\Plugins\FTP\Hosts
- HKCU\Software\Far2\Plugins\FTP\Hosts

```
.text:0040F0B9                 push    3E8h            ; dwBytes
.text:0040F0BE                 call    AllocateMemory_IntializeToZero
.text:0040F0C3                 mov     dword_49FA48, eax
.text:0040F0C8                 pop     ecx
.text:0040F0C9                 test    eax, eax
.text:0040F0CB                 jz      short loc_40F114
.text:0040F0CD                 push    esi
.text:0040F0CE                 push    edi
.text:0040F0CF                 push    1
.text:0040F0D1                 mov     edi, HKEY_CURRENT_USER
.text:0040F0D6                 mov     esi, offset sub_40EF92
.text:0040F0DB                 push    edi
.text:0040F0DC                 push    esi
.text:0040F0DD                 push    offset aSoftwareFarPlu ; "Software\\Far\\Plugins\\FTP\\Hosts"
.text:0040F0E2                 call    StealDataFromRegistry
.text:0040F0E7                 push    1
.text:0040F0E9                 push    edi
.text:0040F0EA                 push    esi
.text:0040F0EB                 push    offset aSoftwareFar2Pl ; "Software\\Far2\\Plugins\\FTP\\Hosts"
.text:0040F0F0                 call    StealDataFromRegistry
.text:0040F0F5                 push    0
.text:0040F0F7                 push    0
.text:0040F0F9                 push    dword_49FA48
.text:0040F0FF                 call    AddDataToPacket
.text:0040F104                 push    dword_49FA48    ; lpMem
.text:0040F10A                 call    ZeroInitialisation_heapFree
.text:0040F10F                 add     esp, 30h
.text:0040F112                 pop     edi
.text:0040F113                 pop     esi
.text:0040F114
.text:0040F114 loc_40F114:                             ; CODE XREF: StealFromRegistry_FTP+12↑j
.text:0040F114                 push    1               ; int
.text:0040F116                 push    0               ; __int16
.text:0040F118                 push    offset aSFarManagerPro ; "%s\\Far Manager\\Profile\\PluginsData\\"..
.text:0040F11D                 call    sub_412182
.text:0040F122                 xor     eax, eax
.text:0040F124                 add     esp, 0Ch
.text:0040F127                 inc     eax
.text:0040F128                 retn
.text:0040F128 StealFromRegistry_FTP endp
.text:0040F128
```

شکل ۵. سرقت از رجیستری Far2 .

به محض اینکه Dyzap آنها را پیدا کند، شروع به جستجوی مقادیر کلیدهای فرعی برای "Password"، "User"، و "HostName" می‌کند. لیستی از برنامه‌هایی که ممکن است با استفاده از رجیستری‌شان مورد هدف قرار گیرند، در جدول زیر نشان داده شده است. در گام بعدی، بدافزار به ازای هر برنامه‌ای، بصورت کد سخت در مسیر رجیستری -که ممکن است حاوی اطلاعات محرمانه باشد- نوشته می‌شود.

جدول ۱. برنامه‌هایی که بدافزار سعی در سرقت اطلاعات آنها از طریق رجیستری‌شان دارد.

نام برنامه	رجیستری
QtWeb.NET	"Software\QtWeb.NET\QtWeb Internet Browser\AutoComplete"
LinasFTP	"Software\LinasFTP\Site Manager"
NCH Software	"Software\NCH Software\Fling\Accounts" "Software\NCH Software\ClassicFTP\FTPAccounts"
9bis.com	"Software\9bis.com\KiTTY\Sessions"
SimonTatham	"Software\SimonTatham\PuTTY\Sessions"
IncrediMail Martin Prikryl	"Software\IncrediMail\Identities" "Software\Martin Prikryl"
WinChips	"Software\WinChips\UserAccounts"
Microsoft Outlook	"Software\Microsoft\Windows NT\CurrentVersion\Windows Messaging Subsystem\Profiles\Outlook" "Software\Microsoft\Office\15.0\Outlook\Profiles\Outlook" "Software\Microsoft\Office\16.0\Outlook\Profiles\Outlook"

Pidgin

یکی دیگر از قابلیت‌های Dyzap، سرقت اطلاعات محرمانه از فایل‌هایی است که اطلاعات ورودی حساب‌هایی که روی سیستم آلوده قرار دارند را ذخیره می‌کنند. برای نمونه می‌توان برنامه‌ی Pidgin را نام برد که یک برنامه گفتگوست. این برنامه به کاربر این امکان را می‌دهد که بطور همزمان به چندین حساب کاربری از شبکه‌های گفتگوی مختلف وارد شود. این برنامه اطلاعات ورود به حساب‌ها را داخل یک فایل XML در مسیر "%AppData%\Roaming\.purple\accounts.xml." ذخیره می‌کند. بدافزار Dyzap با جستجوی مسیرهای ممکن، تلاش می‌کند فایل با پسوند xml را بیابد و از آن کپی می‌گیرد تا بعداً به سرور C & C خودش ارسال کند.

مسیرهای ممکن برای یافتن فایل هدف در شکل زیر آمده است.

```
.text:0041208B ; ---------------------------------------------------------------------------
.text:0041208B
.text:0041208B loc_41208B:                             ; CODE XREF: LookUpFileInSpecificPath+91↑j
.text:0041208B                 mov     ax, [ebp+arg_C]
.text:0041208F                 push    esi
.text:00412090                 push    edi
.text:00412091                 xor     edi, edi
.text:00412093                 inc     edi
.text:00412094                 test    ax, ax
.text:00412097                 jnz     short loc_4120A2
.text:00412099                 push    CSIDL_APPDATA
.text:0041209B
.text:0041209B loc_41209B:                             ; CODE XREF: LookUpFileInSpecificPath+30↓j
.text:0041209B                                         ; LookUpFileInSpecificPath+3A↓j ...
.text:0041209B                 call    CallSHGetFolderPath
.text:004120A0                 jmp     short loc_4120F6
.text:004120A2 ; ---------------------------------------------------------------------------
.text:004120A2
.text:004120A2 loc_4120A2:                             ; CODE XREF: LookUpFileInSpecificPath+1E↑j
.text:004120A2                 cmp     ax, di
.text:004120A5                 jnz     short loc_4120AB
.text:004120A7                 push    CSIDL_PROFILE
.text:004120A9                 jmp     short loc_41209B
.text:004120AB ; ---------------------------------------------------------------------------
.text:004120AB
.text:004120AB loc_4120AB:                             ; CODE XREF: LookUpFileInSpecificPath+2C↑j
.text:004120AB                 cmp     ax, 2
.text:004120AF                 jnz     short loc_4120B5
.text:004120B1                 push    CSIDL_MYDOCUMENTS
.text:004120B3                 jmp     short loc_41209B
.text:004120B5 ; ---------------------------------------------------------------------------
.text:004120B5
.text:004120B5 loc_4120B5:                             ; CODE XREF: LookUpFileInSpecificPath+36↑j
.text:004120B5                 cmp     ax, 3
.text:004120B9                 jnz     short loc_4120BE
.text:004120BB                 push    ebx
.text:004120BC                 jmp     short loc_41209B
.text:004120BE ; ---------------------------------------------------------------------------
.text:004120BE
.text:004120BE loc_4120BE:                             ; CODE XREF: LookUpFileInSpecificPath+40↑j
.text:004120BE                 cmp     ax, 4
.text:004120C2                 jnz     short loc_4120C8
.text:004120C4                 push    CSIDL_COMMON_APPDATA
.text:004120C6                 jmp     short loc_41209B
.text:004120C8 ; ---------------------------------------------------------------------------
.text:004120C8
.text:004120C8 loc_4120C8:                             ; CODE XREF: LookUpFileInSpecificPath+49↑j
.text:004120C8                 cmp     ax, 5
.text:004120CC                 jnz     short loc_4120D2
.text:004120CE                 push    CSIDL_PROGRAM_FILES
.text:004120D0                 jmp     short loc_41209B
.text:004120D2 ; ---------------------------------------------------------------------------
.text:004120D2
.text:004120D2 loc_4120D2:                             ; CODE XREF: LookUpFileInSpecificPath+53↑j
.text:004120D2                 cmp     ax, 6
.text:004120D6                 jnz     short loc_4120DC
```

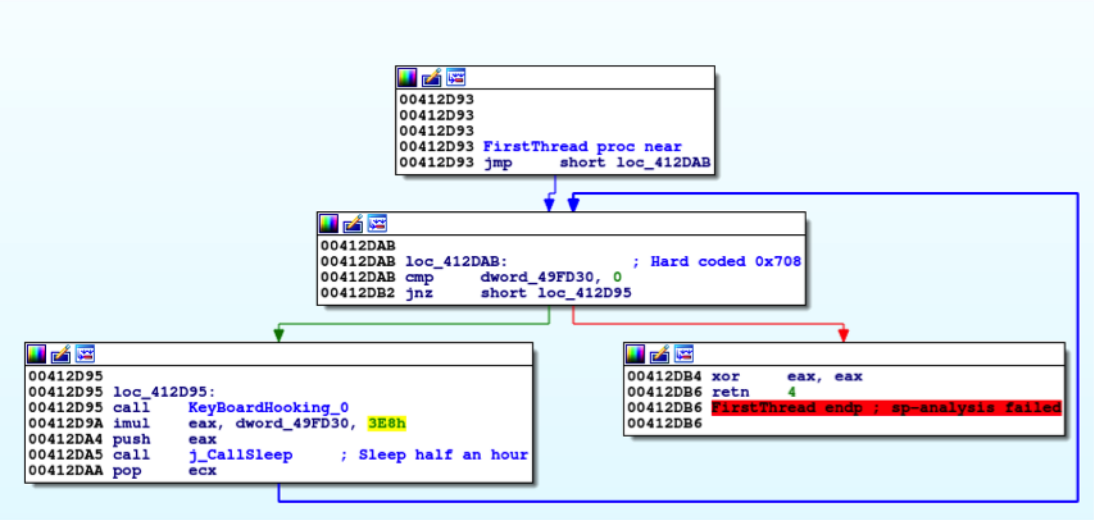
در ادامه لیستی از همگی برنامه‌ها و فایل‌های مربوطه‌شان که این بدافزار در آنها به دنبا لاطلاعات محرمانه می‌گردد، در قالب جدول آمده است.

مرکز ماهر

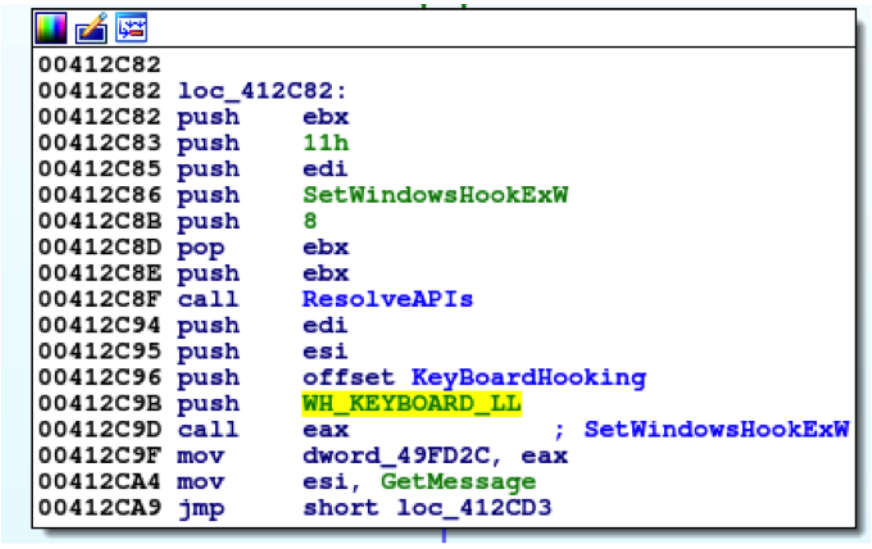
رجیستری	نام برنامه
"\QupZilla\profiles\default\browsedata.db"	QupZilla
"\FTPShell\ftpshell.fsi"	FTPShell
"\Notepad++\plugins\config\NppFTP\NppFTP.xml"	Notepad++
"\oZone3D\MyFTP\myftp.ini"	Ozone3D
"\FTPBox\profiles.conf"	FTPBox
"\FTP Now\sites.xml"	FTP Now
"\NexusFile\ftpsite.ini"	NexusFile
"\.config\fullsync\profiles.xml"	Unknown [.config]
"\FTPInfo\ServerList.xml" "\FTPInfo\ServerList.cfg"	FTPInfo
"\FileZilla\Filezilla.xml" "\FileZilla\filezilla.xml" "\FileZilla\recentservers.xml" "\FileZilla\sitemanager.xml"	FileZilla
"\Staff-FTP\sites.ini"	Staff-FTP
"\BlazeFtp\site.dat"	BlazeFtp
"\GoFTP\settings\Connections.txt"	GoFTP
"\Estsoft\ALFTP\ESTdb2.dat"	Estsoft
"\DeluxeFTP\sites.xml"	DeluxeFTP
"\GHISLER\wcx_ftp.ini"	GHISLER
"\FTPGetter\servers.xml"	FTPGetter
"\WS_FTP\WS_FTP.INI" "\WS_FTP.INI"	WS_FTP
"\site.xml"	[Unknown]
"\Steed\bookmarks.txt"	Steed
"\INSoftware\NovaFTP\NovaFTP.db"	INSoftware
"\NetDrive\NDSites.ini" "\NetDrive2\drives.dat"	NetDrive
"\Far Manager\Profile\PluginsData\42E4AEB1-A230-44F4-B33C-F195BB654931.db"	Far Manage
"\FreshWebmaster\FreshFTP\FtpSites.SMF"	FreshWebmaster
"\BitKinex\bitkinex.ds"	BitKinex
"\UltraFXP\sites.xml"	UltraFXP
"\Odin Secure FTP Expert\QFDefault.QFQ" "\Odin Secure FTP Expert\SiteInfo.QFP"	Odin Secure FTP Expert
"\Pocomail\accounts.ini"	Pocomail
"\GmailNotifierPro\ConfigData.xml"	GmailNotifierPro
"\WinFtp Client\Favorites.dat" "\32BitFtp.TMP"	WinFtp Client 32BitFtp
"\FTP Navigator\Ftplist.txt"	Navigator
"\Opera Mail\Opera Mail\wand.dat"	Opera Mail
"\yMail2\POP3.xml" "\yMail2\SMTP.xml" "\yMail2\Accounts.xml" "\yMail\ymail.ini"	yMail2
"\TrulyMail\Data\Settings\user.config"	TrulyMail
"\To-Do DeskList\tasks.db"	To-Do DeskList
"\Conceptworld\Notezilla\Notes8.db"	Conceptworld
"\Microsoft\Sticky Notes\StickyNotes.snt"	Microsoft

ویژگی کی‌لاگر.

بدافزار Dyzap در مولفه‌ی کی‌لاگر خود، نخ جدیدی برای بدست آوردن همه‌ی ورودی‌های صفحه کلید، داده‌های Clipboard، و عناوین پنجره‌ها ایجاد می‌کند. این روند در شکل ۷ نشان داده شده است. اطلاعات به سرقت رفته، همگی در فایلی ذخیره می‌شوند که توسط بدافزار با %RANDOM-NUMBER%.kdb داخل یک پوشه‌ی موقت ایجاد می‌شود. بدافزار Dyzap برای به دام انداختن صفحه کلید، روال SetWindowsHookExW() را فراخوانی می‌کند تا ورودی صفحه کلید را بدست بیاورد. نتیجه‌ی بدست آمده توسط کی‌لاگر نیز بهمراه دیگر اطلاعات به سرقت رفته، به سرور C & C بارگزاری می‌شود.



شکل ۷. نخ ایجاد شده برای به دام انداختن صفحه کلید.



شکل۸. روال چنگک که رخدادهای ورودی در سطح پایین صفحه کلید را دیده‌بانی می‌کند.

ارتباط با سرور C & C .

پس از جمع‌آوری اطلاعات از برنامه‌های مورد هدف، بسته‌ای از اطلاعات به سرقت رفته فراهم می‌شود. داده با ساختار دودویی مرتب شده به سرور C & C ارسال می‌شود. ساختار بسته شامل سه زیرساختار اصلی است. که هر قطعه اطلاعات در یکی از این بخش (بلاک)ها نشانده می‌شود. این بلاک‌ها در جدول ۲ نشان داده شده‌اند.

جدول ۲. ساختارهای پایه‌ی بلاک‌ها.

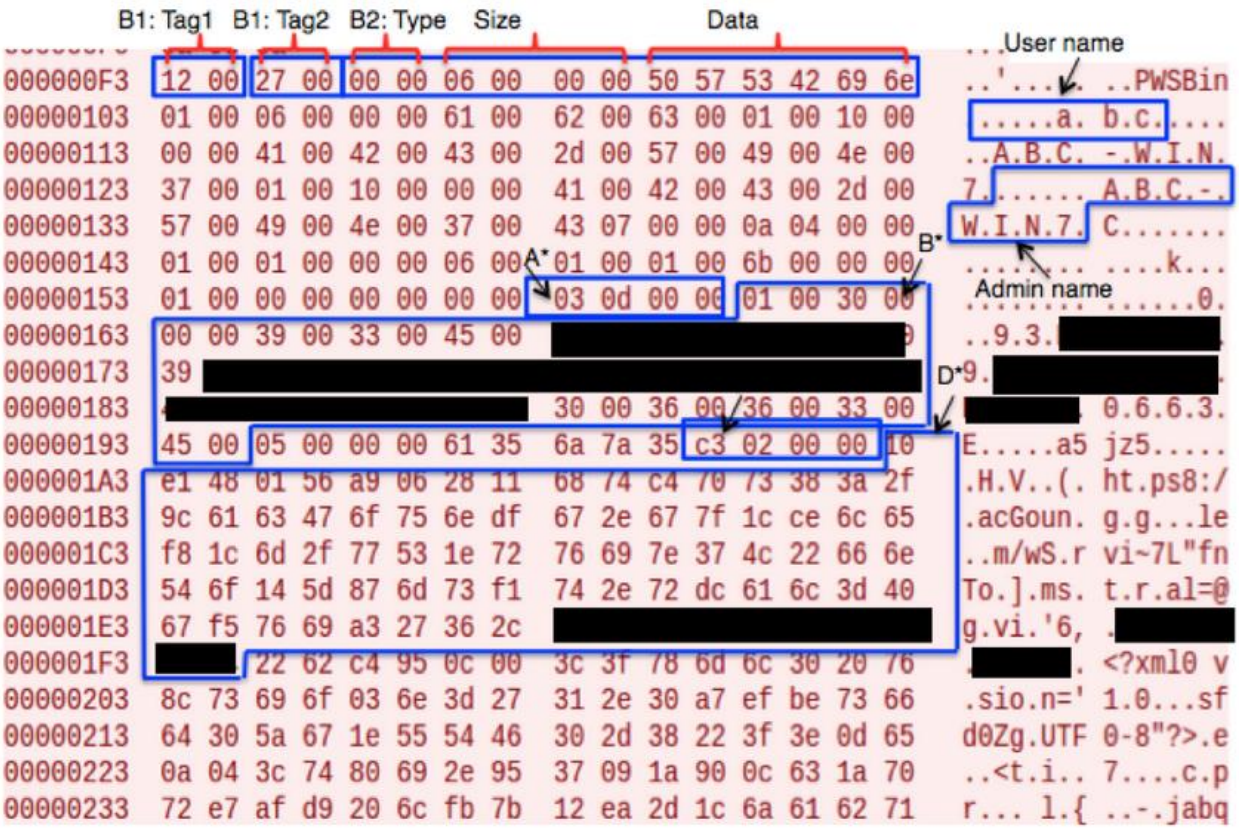
struct Block_1 {
WORD tag;
}
	hard coded tags

struct Block_2 {
WORD data_type;
DWORD data_size;
BYTE data[];
}
	data_type - 00 or 01 to indicate the nickname is Unicode or Ascii
	data_size - Size of following data

struct Block_3{
DWORD data_size;
BYTE data[];
}
	data_size - Size of following data

اطلاعات بسته‌بندی شده، با تگ‌های کد سخت شروع می‌شوند. هه‌ی تگ‌های نشانده شده در بلاک ۱ در شکل ۹ تحت عنوان B1 نشان داده شده‌اند. برای نمونه 0x12 و 0x27 در بسته تحت عنوان x12\x00\x27\x00 ظاهر می‌شود. سپس یک رشته‌ی کد سخت، "PWSBin" به تگ‌های موجود در ساختار بلاک ۲ اضافه شده است.

سپس در بسته‌ی مذکور، *A قرار می‌گیرد که اندازه‌اش ۴بیت است، داده‌ی به سرقت رفته را نمایش می‌دهد و توسط بدافزار رمزنگاری شده است.در پایان نیز داده‌ی به سرقت رفته و رمزگذاری شده به همراه اندازه‌اش(*C و*D)، با ساختار بلاک ۳ به بسته اضافه خواهند شد. قابل توجه است که هر بخش از داده‌ی به سرقت رفته، با بایتی آغاز می‌شود که شاخصی از لیست شاخص‌ها را نشان می‌دهد که اشاره به برنامه‌ی مربوطه دارد.



شکل ۹. محتوای درخواست HTTP ارسال شده به سرور.

جدول ۴. خلاصه‌ی تبادلات در سرور فرمان و کنترل.

بخش	ساختار	بخش	ساختار

01	struct Register{
	WORD tag1 ;
	WORD tag2;
	WORD nickname1_type;
	DWORD nickname1_size;
	BYTE nickname1[6];
	}
		06	struct Tags{
			WORD tag3;
			WORD tag4;
			WORD tag5;
			WORD tag6;
			}

02	struct StealUserName{
	WORD UserName_type;
	DWORD UserName_size;
	BYTE UserName[];
	}
		07	struct OriginalStolenSize{
			DWORD SizeOfStolenInfo ;
			}

03	struct StealPCName{
	WORD PCName_type;
	DWORD PCName_size;
	BYTE PCName[];
	}
		08	struct Mutex{
			WORD Mutex_type;
			DWORD Mutex_size;
			BYTE MutexName[];
			}

04	struct StealDomainName{
	WORD DomainName_type;
	DWORD DomainName_size;
	BYTE DomainName[];
	}
		09	struct NickName2{
			WORD nickname2_type;
			DWORD nickname2_size;
			BYTE nickname2[5];
			}

05	struct StealPCInfo{
	WORD SePrivilegeIsSet;
	WORD SIDIsSet;
	WORD ProcessorIsAMD64;
	WORD MajorVersion;
	WORD MinorVersion;
	WORD ProductType;
	WORD Pre_initialized;
	}
		10	struct StolenInfo{
			WORD StolenInfo_size;
			BYTE StolenInfo[];
			}

نتیجه گیری.

Dyzap یک بدافزار چندمنظوره‌است که تنها به یک راه برای سرقت اطلاعات محدود نمی‌شود. نه فایل‌های محلی نصب شده‌ی برنامه‌ها و نه رجیستری آنها از خطر این بدافزار در امان نمی‌باشند. Dyzap نه تنها اطلاعاتی از برنامه‌ها جمع‌آوری می‌کند، همینطور نسبت به اطلاعات ورودی صفحه کلید شما نیز کنجکاو است و آنها را نیز جمع‌آوری می‌کند. نسخه‌ای که هم‌اکنون فعال است، توانایی کافی برای دزدی از تعداد بسیار زیادی از برنامه‌ها را دارد. در این مطلب نشان دادیم که سرقت داده‌ها چگونه اتفاق می‌افتد، و نیز چگونه این بدافزار همه‌ی اطلاعات جمع‌آوری شده را قبل از ارسال به سرور فرمان و کنترل خود، به شکل دودویی مرتب درمی‌آورد.