ابزار های هک

مهسا قنبري

Backorificeيک برنامه کاربردي سرويس‌دهنده / سرويس‌گيرنده است که به نرم‌افزار سرويس‌گيرنده اجازه نظارت، مديريت و اجراي ديگر اعمال چندرسانه‌ايي و شبکه را بر روي ماشيني که در حال اجراي سرويس‌دهنده است، مي‌دهد. براي ارتباط برقرارکردن با سرويس‌دهنده، متن و يا سرويس‌گيرنده gui مي‌توانند بر روي هر ماشين ويندوز مايکروسافت به اجرا دربيايند. سرويس‌دهنده بطور متداول فقط در ويندوز ۹۵/۹۸ اجرا مي‌شود.

Backorificeشامل ۶ فايل است:

- **boserve.exe :** سرویس‌دهنده **Backorifice** که بصورت خودکار نصب مي‌شود.
- **bogui.exe :** سرویس گیرنده **Backorifice, gui**
- **boclient.exe :** سرویس گیرنده متن **orifice Back**
- **boconfig.exe :** ابزاري براي پيكربندي **exename**، پورت ، **password** و **plugin** پيش فرض براي يک **Boserver.**
- **melt.exe : Decompress** کردن فايلهاي فشرده شده با فرمان **File freeze.**
- **freez.exe :** فشرده‌کردن فايلهايي كه مي‌توانند با فرمان **decompress**، **Filemelt** شوند.

براي نصب سرويس‌دهنده، تنها لازم است كه سرويس‌دهنده اجرا شود. زماني كه سرويس‌دهنده اجرا مي‌گردد، سرويس‌دهنده خودش

نصب و سپس حذف مي‌شود. اين مسئله براي محيطهاي شبكه بسيار مفيد است، زيرا سرويس‌دهنده مي‌تواند به سادگي با كپي كردن فايل اجرايي سرويس‌دهنده در دايركتوري Startup بر روي يک ماشين نصب گردد، بنابراين فايل اجرايي سرويس‌دهنده ابتدا نصب و سپس حذف خواهد شد. زماني كه سرويس‌دهنده بر روي يک ماشين نصب مي‌گردد، با هر بار راه‌اندازي ماشين، سرويس‌دهنده نيز Start مي‌شود.

براي ارتقاء بخشيدن به Backorifice، running copy از راه دور، به سادگي نسخه جديد سرويس‌دهنده را به ميزبان راه دور Upload كنيد، و براي اجراي آن از فرمان Process spawn استفاده نماييد.

هنگام اجرا، سرويس‌دهنده بطور خودكار تمام برنامه‌هاي در حال اجرا را Kill مي‌كند، خود را بر روي نسخه قديمي نصب مي‌نمايد و خودش

را از موقعيت نصب شده‌اش اجرا و exe به روزرساني شده را حذف مي‌كند.

قبل از نصب، برخي از امكانات سرويس‌دهنده مي‌توانند پيكربندي شوندfilename .ايي كه Backorifice خود نصب مي‌كند، پورتي كه سرويس‌دهنده منتظر شنيدن آن است وpassword اي كه براي رمزگذاري بكار مي‌رود، همگي مي‌توانند با استفاده از boconf.exe ، Utilityپيكربندي شوند. اگر سرويس‌دهنده پيكربندي نشود، در شنيدن پورت ۷۳۳۱۳كوتاهي مي‌كند، براي رمزگذاري از password استفاده نمي‌نمايدpacket) ها هنوز رمزگذاري شده هستند) و خود را بصورت (Space dot exe) "exe. " نصب مي‌كند.

سرويس‌گيرنده از طريقPacket هاي رمزگذاري شده UDP با سرويس‌دهنده ارتباط برقرار مي‌كند. براي يك ارتباط موفق، لازم

است سرویس‌گیرنده‌Packet ها را به همان پورتي که سرویس‌دهنده منتظر شنیدن آن است بفرستد و password سرویس‌گیرنده باید با passwordرمزگذاري که سرویس‌دهنده با آن پیکربندي شده، هماهنگ باشد.

پورتي که سرویس‌گیرنده‌Packet هاي خود را از آنجا مي‌فرستد مي‌تواند با استفاده از P Option- با هر دو سرویس‌گیرنده gui و متن Setشود. اگرPacket ها فیلتر شده باشند یا یک firewall در محل وجود داشته باشد، ممکن است لازم باشدpacket ها از یک پورت خاص فرستاده شوند که فیلتر شده و یا بلوکه شده نباشند. زماني که ارتباط UDPبدون اتصال باشدPacket ،ها ممکن است در مسیر خود به سرویس‌دهنده و یاPacket هاي برگشتي در مسیر بازگشتشان به سرویس‌گیرنده بلوکه شوند.

عمليات با فرستادن فرمانهايي از سرويس‌گيرنده به يک آدرس خاص

IPبر روي سرويس‌دهنده به اجرا درمي‌آيند. اگر ماشين

سرويس‌دهنده روي يک آدرس ايسنا نباشد، مي‌تواند با استفاده از

فرمانهاي Sweep يا Sweeplist از سرويس‌گيرنده متن يا از

سرويس‌گيرنده gui با استفاده از dialog "...ping" و يا با قراردادن

يک IP مقصد ،"*.1.2.3" مستقر گردد. اگر پاک شدن ليستSubnet

ها هنگام پاسخگويي ماشين سرويس‌دهنده صورت گيرد،

سرويس‌گيرنده در دايرکتوري مشابه به عنوان ليست Subnet ظاهر

مي‌گردد و اولين خط از اولين فايل را که با نام فايل subnet يافته است

نمايش مي‌دهد.

فرمانهايي که بطور متداول در Backorifice اجرا مي‌گردند در پايين

ليست شده است. برخي از فرمانها بين سرويس‌گيرنده متن وgui

متفاوت است، اما تقريباً در تمام فرمانها گرامر يكي است. در

سرويس‌گيرنده متن، با تايپ 'help' command اطلاعات بيشتري در

مورد هريک از فرمانها به نمايش درخواهد آمد. زماني كه فرماني از

ليست "Command" انتخاب مي‌شود، سرويس‌گيرنده gui برچسبي از

دو پارامتر را براي توضيح هريک از ابعاد فرمان قرار مي‌دهد. در

صورتي كه بخشي از اطلاعات موردنياز از جانب فرمان ارائه نگردد،

خطاي "missing data" از طريق سرويس‌دهنده بازگردانده خواهد

شد. فرمانهاي Backorifice از اين قرارند:

فرمان(gui/text)

App add/appadd

تكثير يک برنامه كاربردي متني بر روي پورت .TCP اين كار به شما

اجازه مي‌دهد تا برنامه كاربردي متني يا تحت) dos همچون

Command.com(را از طريق يک بخش Telnet كنترل كنيد.

App del/appdel

ارتباط يک برنامه كاربردي را متوقف مي‌كند.

Appslist/applist

برنامه‌هاي كاربردي را كه بطور متداول براي برقراري ارتباط به كار

مي‌روند، ليست مي‌كند.

Directory Create/md

يک دايركتوري ايجاد مي‌كند.

Directory list/dir

فايلها و دايركتوري را ليست مي‌كند. اگر بخواهيد بيش از يک فايل را

ليست كنيد بايد يک كاراكتر جانشين معين كنيد.

Directory remove/rd

يک directory را پاک مي‌كند.

Export add/shareadd

يک export روي Server ايجاد مي‌كند. دايركتوري export شده يا

آيكن درايو با آيكن shared hand نمايش داده نمي‌شود.

Export delete/sharedel

exportرا حذف مي‌كند.

Exports list/sharelist

نام اشتراکهاي متداول، درايو يا دايرکتوري که به اشتراک گذاشته

شده‌اند، دستيابي به آن اشتراک و password براي اشتراک را ليست

مي‌کند.

FileCopy/Copy

فايل را کپي مي‌کند.

File delete/del

فايل را حذف مي‌کند.

FileFind/Find

درخت دايرکتوري را بدنبال فايلهايي که با مجموعه مشخصات جانشين

هماهنگ است جستجو مي‌کند.

Filefreeze/freeze

يک فايل را فشرده مي‌کند.

filemelt/melt

يک فايل را Decompress مي‌کند.

Fileview/view

محتواي يک فايل متن را مشاهده مي‌کند

HTTP Disable/httoff

سرويس‌دهنده http را غيرفعال مي‌سازد.

Keylog begin/keylog

Keystorkeها را روي ماشين سرويس‌دهنده به يک فايل متن log

مي‌کند. اين log به شما نام پنجره اين را که متن در آن تايپ شده را

نشان مي‌دهد.

Keylog end

loggingصفحه کليد را به پايان مي‌رساند. براي پايان دادنlogging

صفحه کليد از سرويس‌گيرنده متن از 'keylog stop' استفاده کنيد.

mm capture aui/capavi

ويدئو و صدا را (در صورت موجود بودن) از وسيله ورودي ويدئو به

يک فايل aui ضبط مي‌کند.

mm capture Frame/copframe

تصوير ويدئو را از وسيله ورودي ويدئو به يک فايل bitmap ضبط

مي‌کند.

mm capture screen/capscreen

تصويري از صفحه نمايش ماشين سرويس‌دهنده را به يک فايل

bitmapضبط مي‌کند.

mm List capture devices/listcaps

وسايل ورودي ويدئو را ليست مي‌كند.

mm play sound/sound

يک فايل WAV را روي ماشين سرويس‌دهنده play مي‌كند.

Net connections/netlist

ارتباطات ورودي و خروجي شبكه را ليست مي‌كند.

Net delete/netdisconnect

ارتباط ماشين سرويس‌دهنده را از يک منبع شبكه قطع مي‌كند.

Net use/netconnect

ارتباط ماشين سرويس‌دهنده را با يک منبع شبكه برقرار مي‌سازد.

Net view/netview

تمام رابطهاي شبكه، حوزه‌ها، سرويس‌دهنده‌ها و export هاي قابل

مشاهده از ماشين سرويس‌دهنده را مشاهده مي‌كند.

pinghost/ping

ماشين ميزبان را ping مي‌كند. نام ماشين و شماره نسخه BO را

بازمي‌گرداند.

plugin execute/plugin exeC

pluginيک Backorifice را اجرا مي‌كند. اجراي اعمالي كه با رابط

pluging Backorificeمطابق نباشد ممكن است موجب مختل شدن

سرويس‌دهنده گردد.

Pluging kill/pluginkill

به يک plugin خاص مي‌گويد كه shutdown شود.

plugins list/pluginlist

pluginهاي فعال را ليست مي‌كند و يا مقدار يک plugin را كه خارج

شده است، بازمي‌گرداند.

Process list/proclist

فرآيندهاي اجرايي را ليست مي‌كند.

Process spawn/procspawn

برنامه را اجرا مي‌كند. اگر پارامتر دوم مشخص شده باشد، فرآيند

بصورت يک فرآيند عادي و ديداري اجرا مي‌گردد. در غيراينصورت

فرآيند بصورت پنهاني و يا جدا اجرا مي‌شود.

Redir add/rediradd

ارتباطات TCP ورودي و يا packet هاي udp را به آدرس ديگر ip

تغيير مسير مي‌دهد.

Redir del/redirdel

تغيير مسير يک پورت را متوقف مي‌سازد.

Redir list/redirlist

تغيير مسيرهاي پورت فعال را ليست مي‌كند.

Reg Create key/regmakekey

در registry يک كليد ايجاد مي‌كند.

توجه: در مورد تمام فرمانهاي registry، registry براي مقادير registry،

مقدار \\را قرار ندهيد.

Regdelete key/regdelkey

يک كليد را از registry حذف مي‌كند.

Regdelete value/regdelval

يک مقدار را از registry حذف مي‌كند.

Reglist keys/reglistkeys

كليدهاي فرعي يک كليد registry را ليست مي‌كند.

Reg list values/reglistvals

مقادير يک کليد registry را ليست مي‌کند.

Reg set value/regsetval

براي کليد registry مقداري را قرار مي‌دهد. مقادير برحسب نوعي که بدنبال کاما (،) آمده است و سپس داده‌هاي مقدار تعيين مي‌شوند.

در مورد مقادير باينري (نوع B)، مقدار يکسري از مقادير دو رقمي بر مبناي شانزده است. در مورد مقادير DWORD) نوع D)، مقدار يک عدد دسيمال است. در مورد مقادير رشته‌اي (نوع S)، مقدار يک رشته متني است.

Resolve host/resolve

آدرس ip نام یک ماشین را در رابطه با ماشین سرویس‌دهنده

resolveمي‌کند. نام ماشین مي‌تواند نام یک میزبان اینترنت و یا نام

ماشین یک شبکه محلي باشد.

system dialogbox/dialog

یک کادر مکالمه روي ماشین سرویس‌دهنده با متن تهیه شده و دکمه

'OK'ایجاد مي‌کند. شما مي‌توانید به هر تعداد که مي‌خواهید کادر

مکالمه ایجاد کنید، این کادرها در جلوي کادر قبلي پشت سرهم قرار

مي‌گیرند.

system info/info

اطلاعات سیستم را براي ماشین سرویس‌دهنده نمایش مي‌دهد.

اطلاعات به نمایش در آمده شامل نام ماشین، کاربر جاري، نوع CPU،

حافظه موجود و کلي، اطلاعاتي در مورد نسخه ویندوز و اطلاعاتي در

مورد درايو شامل نوع درايو (ثابت ،cd-rom ،قابل جابه جايي يا راه

دور) و در رابطه با درايوهاي ثابت، اندازه و فضاي خالي درايو

مي‌باشد.

System lockup/lockup

ماشين سرويس‌دهنده را lockup مي‌كند.

System passwords/passes

Passwordهاي Cash شده براي كاربر جاري و password محافظ

صفحه نمايش را نشان مي‌دهدpassword .هاي به نمايش درآمده

ممكن است در آخرشان داده‌هاي اضافه داشته باشند.

System reboot/reboot

ماشين سرويس‌دهنده را Shutdown مي‌كند و مجدد آن را

راه‌اندازي مي‌كند.

TCP file Send/TCPsend

ماشين سرويس‌دهنده را به يک ip و پورت خاص مرتبط مي‌کند و

محتواي فايل مشخص شده را مي‌فرستد و سپس ارتباط را قطع

مي‌کند.

توجه: براي انتقال فايل TCP، آن ip و Port خاص بايد قبل از آنکه

فرمان فايل TCP ارسال و يا fail گردد، شنيده شوند يک Utility

مفيد براي انتقال فايلها netcat است که براي unix و هم براي win32

فايل دسترسي است.

فايلها مي‌توانند با استفاده از فرمان ارسال TCP و netcat با گرامري

شبيه: netcat-1-p666<file از سرويس‌دهنده فرستاده شوند.

فايلها مي‌توانند با استفاده از فرمان دريافت فايل TCP و netcat با

گرامري شبيه: netcat-1-p666>file به سرويس‌دهنده فرستاده

مي‌شوند.

توجه: نسخه netcat ،win32 تا زماني كه به پايان فايل ورودي برسد

خارج و يا قطع ارتباط نمي‌شود. پس از آنكه محتويات فايل منتقل شد ،

netcatرا با ctrl-break يا ctrl-c پايان ببخشيد.

Boconfig:

Boconfig.exeبه شما اجازه مي‌دهد تاOption ها را براي يک

سرويس‌دهنده bo قبل از آنكه نصب شود، پيكربندي كنيد Boconfig .

از شما در مورد نام اجرايي كه نامي است كه Back orifice با آن خود

را در دايركتوري سيستم نصب خواهد كرد، سوال مي‌كند.

ضرورتي ندارد كه Boconfig به exe. ختم شود، اما اگر شما از پسوند فايل استفاده كنيد، Boconfig ، exe. را اضافه نخواهد كرد. سپس در مورد توصيف exe سوال مي‌كند كه در واقع توصيفي است كه exe را در ،registry جايي كه از زمان راه‌اندازي شروع مي‌شود، شرح مي‌دهد. سپس در مورد پورتي كه سرويس‌دهنده از آنجاpaket ها را خواهد شنيد سوال مي‌كند و سپس در موردpassword اي كه براي رمزگذاري از آن استفاده خواهد كرد مي‌پرسد. براي برقراري ارتباط با سرويس‌دهنده با استفاده از سرويس‌گيرنده، سرويس‌گيرنده بايد با همان password مشابه پيكربندي شود. اين نيز مي‌تواند تهي باشد. و بالاخره Boconfig ،در مورد مسير فايل كه مي‌تواند به سرويس‌دهنده متصل شود و در دايركتوري سيستم به عنوانStart هاي سرويس‌دهنده نوشته مي‌شود، سوال مي‌كند. اين مي‌تواند pluginيك Backorifice باشد كه بطور خودكارStart مي‌شود.

سرويس‌دهنده‌اي كه بدون پيكربندي شدن كار مي‌كند، در برقراري ارتباط روي پورت 73313 بدون password دچار نقصان مي‌شود و خود را بصورت "exe." نصب مي‌كند.

مسائل و مشكلات:

صفحه نمايش ضبط MM: bitmap در هر resolution و عمق پيكسلي كه ماشين سرويس‌دهنده در آن اجرا مي‌شود، ذخيره مي‌گردد. در نتيجهbitmap ،ها مي‌توانند با عمقهاي رنگ ۱۶ بيت يا ۲٤ بيت توليد شوند. اكثر برنامه‌هاي كاربردي گرافيكي تنها مي‌توانندbitmap هاي ۸ يا ۳۲ بيتي را اداره كنند و قادر بهload كردن bitmap نيستند و آن را به درستي نشان نمي‌دهند (اين شامل Graphics workshop براي ويندوز WANG Imaging, photoshop توزيع شده با ويندوز

مي‌شود). بهرحال، برنامه Paint.exe كه به همراه Windows مي‌آيد آن را نشان خواهد داد.

loggingصفحه كليد: ظاهراً ويندوز ms-dos فاقد حلقه پيام است كه مانع log شدن كليدهايي مي‌گردد كه درون آنها تايپ مي‌گردد.

تغيير مسير برنامه كاربردي متني -TCP(App add) چندين اشكال وجود دارد. هنگامي كه Command.com باhandle هاي تغيير مسير يافته‌اش ايجاد مي‌شود، سيستم نيز REDIR32.EXE كه تا پايان ارتباط ظاهر نمي‌شود را ايجاد مي‌نمايد.) بنظر مي‌رسد رابط OS كه با مدل Tsrارتباط برقرار مي‌كند در load، dos session مي‌شود تاhandle هاي ورودي و خروجي را به سمتPipe ها تغيير مسير دهد) بنابراين اگر شما ارتباط TCP را قبل از پايان يافتن برنامه كاربردي، پايان ببخشيد (يا آن را خارج كنيد REDIR32.EXE ،و

WINOA386.MOD (' برنامه كاربردي قديمي' (۱۶ بيتي (

wrapper) به اجرا شدن ادامه خواهد داد و Backorifice و سيستم

عامل قادر به پايان بخشيدن آنها نخواهند بود. اين مسئله مانع

shutdown سيستم نيز مي‌شود و هميشه در (Please wait...) باقي

مي‌ماند.

همچنين به نظر مي‌رسد تغيير مسير دادن خروجي از برخي از
و متأسفانه **FTP.EXE** همچون) **Console** برنامه‌هاي كاربردي
مشكل باشد. **boclient.exe)**