باسمه تعالی

بدافزار Phorpiex

معرفی بدافزار

اخیراً کاربران شبکه اینترنت درگیر باج‌افزاری به نام Gandcrab بودند که از طریق ایمیل منتشر می‌شد. این باج‌افزار و بسیاری از بدافزارهای دیگر از خانواده‌ای بدافزاری به نام Phorpiex (یا Trick) برای انتشار خود استفاده می‌کنند. Phorpiex یک بات‌نت است که چندین سال است با استفاده از پروتکل IRC با سرور فرماندهی و کنترل خود ارتباط برقرار می‌کند و فرمان‌های بدخواهانه شامل دانلود سایر بدافزارها، ارسال ایمیل و کرک میل سرور را روی سیستم قربانیان اجرا می‌کند. Phorpiex بدافزار پیشرفته و پیچیده‌ای محسوب نمی‌شود اما به مدت ده سال است که فعال بوده و برای انتشار بسیاری از خانواده‌های بدافزاری مورد استفاده قرار گرفته است.

تحلیل برخی از بدافزارهای این خانواده نشان دهنده آن است که مشخصات فایل pdb این بدافزار که در زمان کمپایل تولید شده در رشته‌های برنامه موجود است. این رشته (C:\Users\x\Desktop\Home\Code\Trik v۶.۰ - WORK - doc\Release\Trik.pdb) در بسیاری از بدافزارها که مربوط به سال‌های اخیر بوده‌اند قابل مشاهده است و به نظر می‌رسد این بدافزارها نیز توسط توسعه دهنده این خانواده بدافزاری توسعه داده شده‌اند. نکته قابل توجه این است که اخیراً بدافزارهای دارای رشته مذکور با تکرار بالایی در سایت virustotal بارگذاری شده‌اند که نشان دهنده آن است که احتمالاً این بدافزار به تازگی در کمپین‌های فعال بدافزاری در حال استفاده شدن است.

گزارش تحلیل

بررسی این بدافزار نشان دهنده آن است که بدافزار کد خود را مبهم‌سازی نکرده است. در اولین مرحله پس از اجرا شدن، بدافزار نسخه‌ای از خود را با یکی از نام‌های winsvc.exe، Winsrvc.exe، winmgr.exe ، Winsam.exe یا Windsrcn.exe در یکی از سه دایرکتوری زیر کپی می‌کند:

- C:\Windows
- C:\Users\$USERNAME\%TEMP%
- C:\Users\$USERNAME\

بدافزار از روش‌های ساده‌ای برای گریز از تشخیص داده شدن و تحلیل استفاده کرده است. برای نمونه در صورتی که پردازه‌های زیر در سیتم در حال اجرا باشند، بدافزار به فعالیت خود خاتمه می‌دهد:

- tcpview.exe
- procmon.exe
- netstat.exe
- wireshark.exe

همچنین بدافزار با روش‌های ساده‌ای اجرا شدن در سندباکس، ماشین مجازی و دیباگ شدن را تشخیص می‌دهد.

در ادامه بدافزار درون دایرکتوری که برای کپی کردن خود انتخاب کرده است، یک زیردایرکتوری با نام M- ۵۰۵۰۵۰۲۶۵۲۸۶۵۸۰۴۲۰۵ ایجاد می‌کند. این نام در نسخه‌های مختلف متغیر است اما الگوی کلی این نام به صورت M- به همراه ۱۹ عدد در ادامه است.

در صورتی که بدافزار برای اولین بار در سیستم اجرا شده باشد، برای کسب ماندگاری در سیستم کلیدی در رجیستری به نام Microsoft Windows Service در مسیر HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run ایجاد می‌کند و نام فایل اولیه‌ای که از خود کپی کرده است (برای نمونه "%USERPROFILE%\M-۱-۵۲-۵۷۸۲-۸۷۵۲-۵۲۴۵\winsvc.exe) را به عنوان مقدار آن تنظیم می‌کند.

ارتباط با سرور فرماندهی و کنترل

نمونه‌های تحلیل شده از یک سرور فرماندهی و کنترل ثابت که درون کد برنامه هاردکد شده بود استفاده کرده‌اند. این سرور در آدرس ۱۸۵.۱۸۹.۵۸.۲۲۲ قرار گرفته است. بدافزار برای ارتباط با این سرور از یک بات IRC روی پورت ۵۰۵۰ پروتکل TCP استفاده می‌کند. نام کاربری بات IRC به فرمت |<۳ character Country Code>|[a-z] است. وقتی این بات به سرور متصل می‌شود دستوری برای اتصال به یک کانال خاص دریافت می‌کند. در نمونه‌های تحلیل شده نام این کانال #QC یا #SMTP بوده است اگرچه این نام در کمپین‌های مختلف متغیر است. سپس بدافزار از طریق این کانال فرمان‌هایی از مدیران بات‌نت برای شروع ارسال ایمیل‌های فیشینگ یا brute force کردن آدرس‌های ایمیل SMTP دریافت می‌کند. همچنین بدافزار می‌تواند به جای دریافت فرمان ارسال فایل از طریق ایمیل، مستقیماً فرمان دانلود و اجرای فایل را دریافت کند. در شکل زیر نمونه‌ای از ترافیک شنود شده این بات‌نت نمایش داده شده است.

```
NICK `|RUS|ndryavvo
USER x "" "x" :x

:001 x.x 001
:002 002 002
:003 003 003
:004 004 004
:005 005 005
:005 005 005
:005 005 005
PING 422 MOTD
JOIN #new (null)
PONG 422
:`|RUS|ndryavvo!x@143.215.130.239 JOIN :#new
:x.x 332 `|RUS|ndryavvo #new :.j #dl .j #up
:x.x 333 `|RUS|ndryavvo #new x 1522481874
JOIN #dl (null)
JOIN #up (null)
:`|RUS|ndryavvo!x@143.215.130.239 JOIN :#dl
:x.x 332 `|RUS|ndryavvo #dl :.d x |108|99|111|113|29|41|56|31|39|55|18|16|10|54|58|44|47|33|42|63|126|83|80|59|103|120|100|
:x.x 333 `|RUS|ndryavvo #dl x 1522482245
:`|RUS|ndryavvo!x@143.215.130.239 JOIN :#up
:x.x 332 `|RUS|ndryavvo #up :.d u |108|99|111|113|29|41|56|31|39|55|18|16|10|54|58|44|47|33|42|63|126|83|80|59|103|120|100|
:x.x 333 `|RUS|ndryavvo #up x 1522482250
```

در این کانال فرمان‌هایی برای متوقف کردن عملیات ارسال ایمیل و brute force کردن SMTP ارسال می‌شود که به ترتیب عبارتند از: "m.off" و "b.off". بدافزار با دریافت فرمان "rmrf" به طور کامل خود را از سیستم قربانی حذف می‌کند.

در صورتی که برای سرور C&C مذکور درخواست HTTP ارسال شود، مشاهده شده که agent های زیر در حال استفاده هستند:

Mozilla/۵.۰ (Macintosh; Intel Mac OS X ۱۰.۹; rv:۲۵.۰) Gecko/۲۰۱۰۰۱۰۱ Firefox/۲۵.۰

یکی از دلایل قابل اعتماد برای آلوده بودن سیستم، ارتباط HTTP از طریق agent فوق با آدرس سرور است.

Brute force کردن SMTP

یکی از اعمال بدخواهانه‌ای که این بدافزار قادر به انجام آن است استفاده از سیستم قربانی برای brute force کردن اکانت‌های SMTP سرورهای ایمیلی است که لیست آن‌ها از طریق سرور فرماندهی و کنترل برای بدافزار ارسال می‌شود. بدافزار پس از دریافت این لیست و دریافت فرمان SMTP Brute Force ترکیبی از نام‌های کاربری و رمز عبور را که در جدول زیر آمده است برای ورود به سرورهای SMTP تست می‌کند.

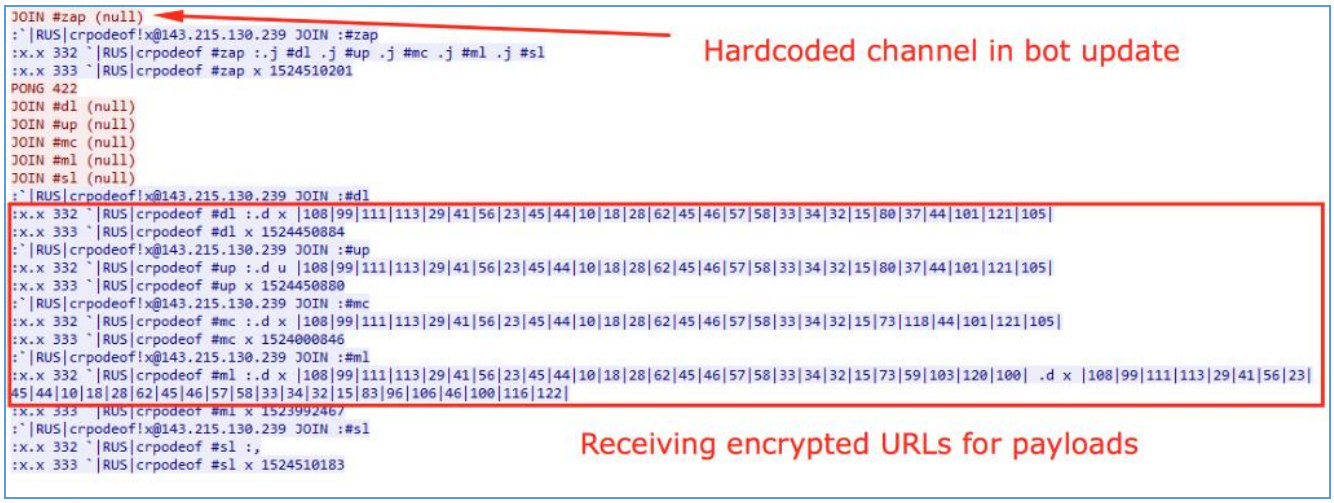
Username/Passwords	Usernames/Passwords
test	guest۱
test۱	guest۱۲۳
test۱۲۳	testing
info	upload
admin	tester
webmaster	testuser۱
postmaster	۱۲۳٤٥
contact	۱۲۳٤٥٦
۱۲۳٤٥	۱۲۳٤٥٦۷
۱۲۳٤٥٦	۱۲۳٤٥٦۷۸
۱۲۳٤٥٦۷	۱۲۳٤٥٦۷۸۹
۱۲۳٤٥٦۷۸	۱۲۳٤٥٦۷۸۹۰
۱۲۳۱۲۳	۱۲۳۱۲۳
test	admin
test۱	admin۱
test۱۲۳	admin۱۲۳
test۱۲۳٤	admin۱۲۳٤
info	administrator
admin	ftpadmin
admin۱	ftpuser
Password۱	guest۱
password	guest۱۲۳
۱q۲w۳e	Password۱
۱q۲w۳e٤r	passw۰rd
q۱w۲e۳r٤	password
postmaster	password۱
admin	q۱w۲e۳r٤
administrator	q۱w۲e۳r٤t٥
test	qwerty
test۱	qwerty۱۲۳
test۱۲۳	temp
user	temp۱۲۳
testuser	test
info	test۱
ftpuser	test۱۲۳
ftpadmin	test۱۲۳٤
support	testing

backup	upload
guest	abc۱۲۳
	۱۲۳qwe
	۱q۲w۳e
	۱q۲w۳e٤r

بنابراین در صورتی که در لاگ‌های mail server ای تلاش‌هایی برای ورود با استفاده از ترکیبی از نام‌های کاربری و رمز عبورهای فوق صورت گرفته است، می‌تواند دلیلی بر تلاش Phorpiex در کرک کردن mail server باشد. همچنین ترافیک حجیم از SMTP از یک کلاینت برای تلاش‌های مکرر در ورود به چندین mail server نشانه دیگری از آلوده شدن سیستم میزبان توسط Phorpiex و انجام یک حمله SMTP Brute Force است.

ساخت و توزیع ایمیل

بدافزار پس از دریافت پیامی خاص مبنی بر ساختن ایمیل همراه با یک URL کدگذاری شده از سمت سرور، در سیستم میزبان شروع به کدگشایی URL مذکور و دریافت فایلی می‌کند که در URL قرار داده شده است. در نهایت این فایل زیپ می‌شود و به ایمیل‌های فیشینگ ضمیمه می‌شود. شکل زیر مبادله این اطلاعات را نمایش می‌دهد.



در اکثر موارد محتوای سرآیند و بدنه ایمیل‌ها از انتخاب تصادفی رشته‌های هاردکد شده یا رشته‌های تصادفی با طولی مشخص ایجاد می‌شود. برای نمونه بدافزار برای موضوع ایمیل، یکی از رشته‌های زیر را انتخاب می‌کند. (پس از علامت # تعدادی رقم به صورت تصادفی قرار می‌گیرند).

```
lpString2       dd offset aDocument     ; DATA XREF: build_smtp_template_403CD0+9E5↑r
                                        ; "Document #"
                dd offset aYourDocument ; "Your Document #"
                dd offset aInvoice      ; "Invoice #"
                dd offset aPaymentInvoice ; "Payment Invoice #"
                dd offset aOrder        ; "Order #"
                dd offset aYourOrder    ; "Your Order #"
                dd offset aPayment      ; "Payment #"
                dd offset aTicket       ; "Ticket #"
                dd offset aYourTicket   ; "Your Ticket #"
                align 8
```

- Document #[۰-۹]{۴}
- Your Document #[۰-۹]{۴}
- Invoice #[۰-۹]{۴}
- Payment Invoice #[۰-۹]{۴}
- Your Order #[۰-۹]{۴}
- Payment #[۰-۹]{۴}
- Ticket #[۰-۹]{۴}
- Your Ticket #[۰-۹]{۴}

محتوای بدنه پیام، متن زیر است که به صورت هارد کد شده در بدافزار قرار گرفته است:

```
; char aDearCustomerTo[]
aDearCustomerTo db 'Dear Customer,',0Dh,0Ah
                                        ; DATA XREF: main_irc_spam_2_403CD0+1055↑o
                db 0Dh,0Ah
                db 'to read your document please open the attachment and reply as soo'
                db 'n as possible.',0Dh,0Ah
                db 0Dh,0Ah
                db 'Kind regards,',0Dh,0Ah
                db 0Dh,0Ah,0
                align 10h
; char aCustomerSuppor[]
aCustomerSuppor db ' Customer Support',0Dh,0Ah
```

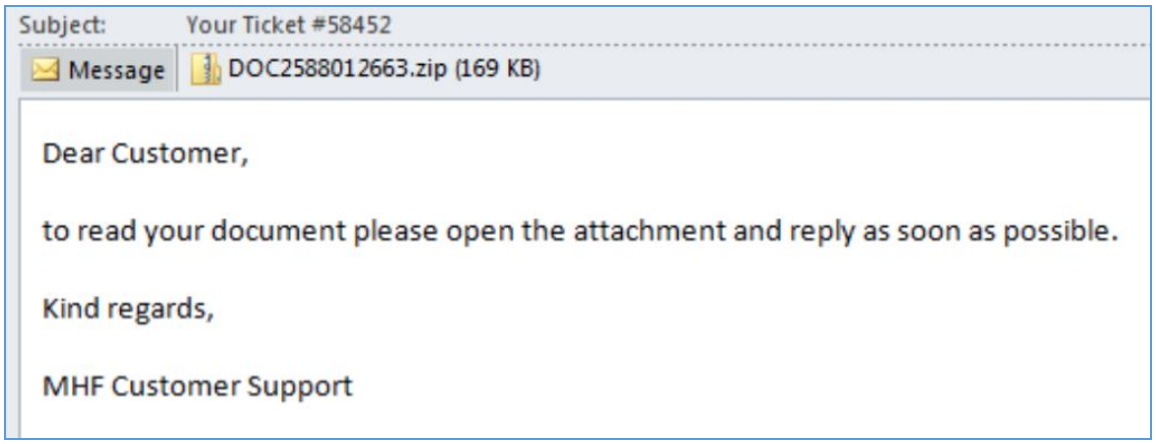
```
push    3
call    gen_random_chars_402FD0
add     esp, 4
push    eax             ; lpsz
call    ds:CharUpperA
push    eax             ; Source
lea     ecx, [ebp+buf]
push    ecx             ; Dest
call    strcat
add     esp, 8
push    offset aCustomerSuppor ; " Customer Support\r\n\r\n"
```

Dear Customer,
to read your document please open the attachment and reply as soon as possible.

Kind regards,

[A-Z]{۳} Customer Support

محتوای نمونه‌ای از ایمیل‌های تولید شده به صورت زیر است:



آنچه که بدافزار در سرآیند ایمیل استفاده می‌کند و نشانه‌های مناسبی برای تشخیص بدافزار است، رشته‌های زیر است:

- Received: from [aA-zZ]{۵} ([[public IP address]]) by [domain] with MailEnable ESMTP; [date]
- Received: (qmail [aA-zZ]{۳} invoked by uid [aA-zZ]{۳}); [date]
- From: [First Name] [Last Name]
- Message-ID: [۰-۹]{۱۴}\.[۰-۹]{۴}\.qmail@[aA-zZ]{۶}]

public IP address که در رشته‌های فوق مشاهده می‌شود، از ارتباط با سرویس IP عمومی api.wipmania.com به‌دست می‌آید. همچنین از سرویس icanhazip.com در این مورد توسط بدافزار استفاده شده است.

انتخاب فرستنده در فرایند ارسال ایمیل

نام و نام خانوادگی فرستنده از نام‌های موجود در جدول زیر انتخاب می‌شود. آدرس ایمیل فرستنده طبق ساختار <hardcoded name in the EXE>[۰-۹]{۲}@[۰-۹]{۴}.com ساخته می‌شود. برای نمونه یکی از آدرس‌های فرستنده که در کمپین توزیع GandCrab مورد استفاده قرار گرفته بود، Bobbie Adams <Bobbie۵۷@۹۲۲۳.com> است.

Names	Names	Names
Adolfo	Deidre	James
Adolph	Deirdre	Baker
Adrian	Delbert	Gonzalez
Adrian	Delia	Nelson
Adriana	Gilda	Carter
Adrienne	Gina	Mitchell
Agnes	Ginger	Perez
Agustin	Gino	Roberts
Ahmad	Giovanni	Turner
Ahmed	Gladys	Phillips
Aida	Glen	Campbell
Aileen	Glenda	Parker
Aimee	Glenn	Evans
Aisha	Glenna	Edwards
Beulah	Gloria	Collins
Beverley	Goldie	Stewart
Beverly	Gonzalo	Sanchez
Bianca	Gordon	Morris
Bill	Hugh	Rogers

Billie	Hugo	Reed
Billie	Humberto	Cook
Billy	Hung	Morgan
Blaine	Hunter	Bell
Blair	Ignacio	Murphy
Blake	Ilene	Jackson
Blanca	Imelda	White
Blanche	Imogene	Harris
Bobbi	Ines	Martin
Bobbie	Tania	Thompson
Bobby	Tanisha	Garcia
Bonita	Tanner	Martinez
Bonnie	Tanya	Robinson
Booker	Tara	Clark
Boris	Tasha	Rodriguez
Boyd	Taylor	Lewis
Brad	Taylor	Walker
Bradford	Teddy	Hall
Bradley	Terence	Allen
Bradly	Teresa	Young
Brady	Teri	Hernandez
Deann	Terra	King
Deanna	Bailey	Wright
Deanne	Rivera	Lopez
Debbie	Cooper	Hill
Debora	Richardson	Scott
Deborah	Howard	Green
Debra	Ward	Adams
Deena	Torres	Smith
Brown	Peterson	Johnson
Davis	Gray	Williams
Miller	Ramirez	Jones
Wilson	Thomas	Wood
Moore	Watson	Barnes
Taylor	Brooks	Ross
Anderson	Kelly	Henderson
Price	Sanders	Coleman
	Bennett	Jenkins

فایلی که در ایمیل ضمیمه می‌شود، از قاعده DOC[۰-۹]{۱۰}.zip برای نام‌گذاری استفاده می‌کند. این فایل در ابتدا از سرور فرماندهی و کنترل دانلود شده و در پوشه فایل‌های موقتی سیستم قرار داده می‌شود. سپس فشرده شده و با استفاده از قاعده فوق، نام‌گذاری می‌شود. در موارد اخیر فایل زیپ شده حاوی یک فایل جاوااسکریپت بدخواه یا یک فایل ورد است که از ماکروها برای رساندن GandCrab و Phorpiex استفاده می‌کند.

علائم کلی آلودگی

IOC	IOC Type	Description
۹۲.۶۳.۱۹۷.۱۰۶:۵۰۵۰	IP Address	Trik/Pony C&C
۱۱۲.۱۲۶.۹۴.۱۰۷:۵۰۵۰	IP Address	Trik C&C
۱۲۳.۵۶.۲۲۸.۴۹:۵۰۵۰	IP Address	Trik C&C
۲۲۰.۱۸۱.۸۷.۸۰:۵۰۵۰	IP Address	Trik C&C
۱۸۵.۱۸۹.۵۸.۲۲۲:۵۰۵۰	IP Address	Trik C&C
auoegfiaefuageudn.ru:۵۰۵۰	Domain	Trik/Pony C&C
۷ba۱۵۰c۸۸۰۸edf۱۸۷a۱ccf۸d۰۵۳۲d۰۷۳۲fff۲bbe۲ ۸f۷۶d۶e۲f۰۲f۸۱۹۶۶۶۹dd۰۶	SHA۲۵۶	Pony sample from May ۱۵th ۲۰۱۸
۰b۴۹۹۶c۰۳b۰۵۹d۱a۱۰۳۴۹f۷۱۵b۶b۲۱ad۹۹۲۶۹۱ ۲faae۸۳۴۵۸۱f۰c۹۶b۲۴ff۱b۳۳f	SHA۲۵۶	Pushdo sample from May ۹th ۲۰۱۸
۹f۳f۸۰۱۶۷c۵d۳۹efb۹e۸۱۵۰۷efec۶d۹bdc۵e۳۱۳۲۳ f۹d۶d۸۹۶۳۰۳۷۴c۷fe۴۹۰f۳۳	SHA۲۵۶	GandCrab sample from May ۹th ۲۰۱۸
ef۱۵۶۳a۹۶۲d۲d۸۶ceb۱dd۰۹۰۵۶f۸۷fcab۴c۳۲e۳ca ۶۴۸۱c۵۱۹۵۰d۳b۶db۴۹d۱۰۸۷	SHA۲۵۶	Trik sample from May ۹th ۲۰۱۸
۵bf۷۹a۱۱۱۴۶۷a۸۵abe۵۷f۱f۳e۹۲f۲۲۷۹b۲۷۷cccae ۵۳ed۲۸c۵۸۴۲۶۷۷۱۷ba۳۷۲f۸	SHA۲۵۶	Trik sample from May ۱۲th ۲۰۱۸
۲۰۳۵ef۰۲a۰۱۴f۹ae۲a۲۱d۳۹c۹۸۶۰۴ca۴۸۶۳d۷۷c ۴۷dcc۱۲d۳۱bb۹b۷b۲d۳e۵fc۹۸	SHA۲۵۶	Trik sample from May ۱۸th ۲۰۱۸
۳df۱۶۲۶۱b۲۸f۳۰۶۸۳dce۶a۶۶۳۳۱۴۵۲f۴ddc۱d۳۴ ۷۲fb۱۹۴ff۵b۵۰۵۲۷۰a۸f۶۴۳۱۱	SHA۲۵۶	Trik sample from May ۱۹th ۲۰۱۸

علائم آلودگی در ایمیل

- **C&C Server:** ۱۸۵.۱۸۹.۵۸[.]۲۲۲

- **Attachments:** DOC[۰-۹]{۱۰}.zip
- **Mail Header:** Received: from [aA-zZ]{۵} ([[public IP address]]) by [domain] with MailEnable ESMTP; [date]
- **Mail Header:** Received: (qmail [aA-zZ]{۳} invoked by uid [aA-zZ]{۳}); [date]
- **Mail Header:** From: [First Name] [Last Name]
- **Mail Header:** Message-ID: [۰-۹]{۱۴}\.[۰-۹]{۴}\.qmail@[aA-zZ]{۶]}
- **Mail Subject:** Document #[۰-۹]{۴}
- **Mail Subject:** Your Document #[۰-۹]{۴}
- **Mail Subject:** Invoice #[۰-۹]{۴}
- **Mail Subject:** Your Order #[۰-۹]{۴}
- **Mail Subject:** Payment #[۰-۹]{۴}
- **Mail Subject:** Ticket #[۰-۹]{۴}
- **Mail Subject:** Your Ticket #[۰-۹]{۴}