اطلاع رسانی عمومی در حوزه افتا

تحلیل باج افزار crysis

۱۳۹۸/۷/۰۲

معرفی باج افزار crysis

باج افزار crysis یک نوع باج افزار است که پرونده‌های سیستم کاربران را رمزگذاری می‌کند و از راه‌های مختلف از قبیل پیوست‌های ایمیل آلوده وارد سیستم کاربران می‌شود. این باج افزار در ابتدا تصویر زیر را به عنوان اطلاع رسانی به کاربران نشان می‌دهد و در ازای رمزگشایی فایل‌های کاربران درخواست بیت کوین می‌کند. این باج افزار در فوریه ۲۰۱۶ وارد فضای مجازی شده است ولی در حال حاضر کلیدهای رمزگشایی این باج افزار برای عموم منتشر شده است.

All your files have been encrypted!

All your files have been encrypted due to a security problem with your PC. If you want to restore them, write us to the e-mail anticrypt@countermail.com
Write this ID in the title of your message CCB90F92
In case of no answer in 24 hours write us to theese e-mails: anticrypt@countermail.com
You have to pay for decryption in Bitcoins. The price depends on how fast you write to us. After payment we will send you the decryption tool that will decrypt all your files.

Free decryption as guarantee

Before paying you can send us up to 1 file for free decryption. The total size of files must be less than 1Mb (non archived), and files should not contain valuable information. (databases,backups, large excel sheets, etc.)

How to obtain Bitcoins

The easiest way to buy bitcoins is LocalBitcoins site. You have to register, click 'Buy bitcoins', and select the seller by payment method and price.
https://localbitcoins.com/buy_bitcoins
Also you can find other places to buy Bitcoins and beginners guide here:
http://www.coindesk.com/information/how-can-i-buy-bitcoins/

پیامدهای منفی بدافزار crysis

- قفل شدن کلیه‌ی پرونده‌های کاربران
- از دسترس خارج شدن کلیه‌ی پرونده‌های مهم و حساس
- درخواست پرداخت بین کوین در ازای ارسال کد رمزگشایی
- خسارت‌های مالی فراوان برای بازگشت اطلاعات و حذف باج افزار
- کند شدن عملکرد کلی سیستم
- عدم تضمین بازگشت اطلاعات بعد از پرداخت باج درخواستی

بررسی فنی باج افزار

- مشخصات فایل آلوده

جدول ۱:اطلاعات کلی باج افزار

File name	Crysis
File type	Ransomware
SHA-1	FFCBA94F675E61F0B84E41163431FE62E8EBA93B
MD5	CDE75B4C59682B1088AC09AFFA8A9D32
File size	94720 (bytes)
Suspicious activity	Encryption files

- عملکرد باج افزار

باج افزار crysis پس فرایند رمزنگاری فایل‌های سیستم با پسوند (.[anticrypt@countermail.com].adobe) دستورالعملی را به کاربر نشان می‌دهد که چگونه در ازای پول پرداختی فایل‌های خود را بازگشایی کند. همچنین، این باج افزار حین رمزگذاری دو فولدر جدول ۲ را از سیستم حذف می‌کند.

جدول۲: فولدرهای حذف شده

C:\ProgramData\Microsoft\Search\Data\Temp\usgthrsvc
C:\Users\All Users\Microsoft\Search\Data\Temp\usgthrsvc

همچنین یک فایل txt بر روی دسکتاپ حاوی پیام زیر را می سازد:

all your data has been locked us

You want to return?

write email anticrypt@countermail.com

- فایل‌های رمزنگاری شده

باج افزار crysis پس از اجرا، تقریباً کلیه‌ی فایل‌های از جمله فایل‌هایی با پسوندهای نشان داده شده در جدول ۳ را در سیستم کاربران رمزنگاری می کند.

جدول ۳: پسوندهای قفل شده

.rar	.db	.H1H	docx	gets	.bin
.ini	.wma	.Lck	.png	.xml	.chk
.DAT	.vdm	.H1Q	html	.cmd	ount
.BAK	.cab	.json	.nsh	vmsg	tore
.cat	.rsm	.GRL	.nsi	.txt	.pat
.inf	conf	.sdf	.zip	.bat	.jpg
.sys	.pem	.log	.url	.vbs	.ico
.dll	.sdi	.jrs	.key	fest	.oem
ts.h	.wim	.000	h-ms	.dtd	.HIST
.exe	d-ms	.001	.LOG1	.xsd	.fbf1
.msi	b-ms	.002	.blf	.SFX	.rred
.ins	wmdb	.DIA	.mp3	.ion	y-ms
.lnk	.wpl	.edb	.wtv	.htm	s-ms
.mui	.etl	.bmp	.wmv	.lst	rget
.H1W	tact	.H1D	Mail	.chm	Link

- سازگاری با سیستم عامل‌ها

این باج افزار با سیستم عامل‌های ویندوز از جمله سیستم عامل‌های نامبرده در جدول ٤ زیر سازگار است.

جدول ٤: سیستم عامل های سازگار

Windows 95 OSR 2/2.1 (Build: 1111) B
Windows NT 4.0 (Build: 1381) Service Pack 1
Windows NT 4.0 (Build: 1381) Service Pack 3
Windows NT 4.0 (Build: 1381) Service Pack 4
Windows NT 4.0 (Build: 1381) Service Pack 6
Windows 98 (Build: 2222) A
Windows ME (Build: 3000)
Windows 2000 (Build: 2195) Service Pack 1
Windows 2000 (Build: 2195) Service Pack 2
Windows 2000 (Build: 2195) Service Pack 3
Windows 2000 (Build: 2195) Service Pack 4
Windows XP (Build: 2600) Service Pack 1
Windows XP (Build: 2600) Service Pack 2
Windows 2003/XPx64 (Build: 3790) Service Pack 1
Windows 2003/XPx64 (Build: 3790) Service Pack 2

- توابع و کتابخانه‌های باج افزار

این باج افزار شامل کتابخانه‌ها و توابع نشان داده شده در جدول ۵ است که تعداد کتابخانه‌ها و توابع برای یک فایل اجرایی سالم غیر قابل قبول است.

جدول ۵: توابع و کتابخانه های سیستمی

KERNEL32	GetProcAddress
	LoadLibraryA
	GetLastError
	WaitForSingleObject
	InitializeCriticalSectionAndSpinCount
	LeaveCriticalSection
	EnterCriticalSection
	ReleaseMutex
	CLOSEhANDLE

توصیه‌های امنیتی برای پیشگیری

- برنامه‌های آگاهی و آموزشی را اجرا کنید. از آنجا که کاربران نهایی اهداف هستند، کارمندان و افراد باید از تهدیدهای باج افزارها و نحوه تحویل آن مطلع باشند.
- فیلترهای Spam قوی را فعال کنید تا ایمیل‌های فیشینگ از رسیدن به کاربران نهایی باز بمانند و ایمیل‌های ورودی را احراز هویت کنند. از فن آوری‌هایی مانند گزارش خط مشی فرستنده (SPF)[1]، گزارش‌های تایید هویت دامنه (DMARC)[2] و DomainKeys Identified Mail (DKIM) برای جلوگیری از جعل ایمیل استفاده کنید.
- تمامی ایمیل‌های دریافتی و خروجی را برای شناسایی تهدیدها و فیلتر کردن فایل‌های اجرایی از رسیدن به کاربران نهایی اسکن کنید.
- پیکربندی فایروال‌ها برای جلوگیری از دسترسی به آدرس‌های مخرب IP شناخته شده راه مؤثری برای حفظ امنیت شبکه است.
- سیستم عامل‌ها، نرم افزارها و فایروال‌های روی سیستم را وصله[3] کنید.

[1] Sender Policy Framework
[2] Domain Message Authentication Reporting and Conformance
[3] Patch

- برنامه‌های ضد ویروس و ضد تروجان را برای انجام اسکن منظم به طور خودکار تنظیم کنید.
- مدیریت استفاده از حساب‌های ممتاز بر اساس اصل حداقل امتیاز: هیچ کاربر نباید دسترسی ممتاز در بالاترین سطح داشته باشد مگر اینکه مورد نیاز باشد و کسانی که نیاز به حساب کاربری مدیر دارند باید از آنها در صورت لزوم استفاده کنند.
- اسکریپت‌های ماکرو را از فایل‌های اداری ارسال شده از طریق ایمیل غیرفعال کنید. با استفاده از نرم افزار Office Viewer برای باز کردن فایل‌های مایکروسافت آفیس از طریق ایمیل به جای برنامه‌های کاربردی full office suite استفاده کنید.
- پیاده سازی سیاست‌های محدودیت نرم افزار (SRP)[4] یا سایر کنترل‌ها برای جلوگیری از اجرای برنامه‌ها از مکان‌های معمول باج افزار صورت گیرد. این پوشه‌ها مانند پوشه‌های موقتی که از مرورگرها و یا برنامه‌های فشرده سازی/آزاد شده از فشردگی، از جمله پوشه AppData / LocalAppData هستند.
- در صورت عدم استفاده از پروتکل از راه دور دسکتاپ [5] (RDP)، آن راغیرفعال کنید.
- استفاده از برنامه لیست سفید، که تنها به سیستم اجازه می‌دهد برنامه‌های شناخته شده و مجاز توسط سیاست امنیتی را اجرا کند.
- برنامه‌های خاص را در یک محیط مجازی و ایزوله اجرا کنید.

[4] Software Restriction Policies
[5] Remote Desktop protocol