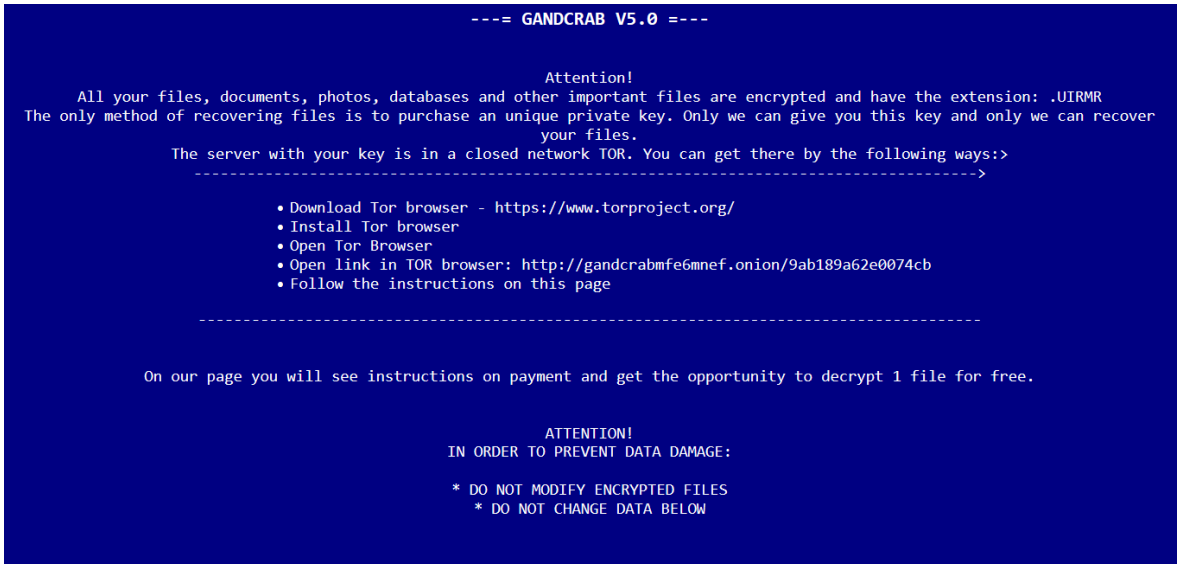
باج‌افزار GandCrab نسخه ۵

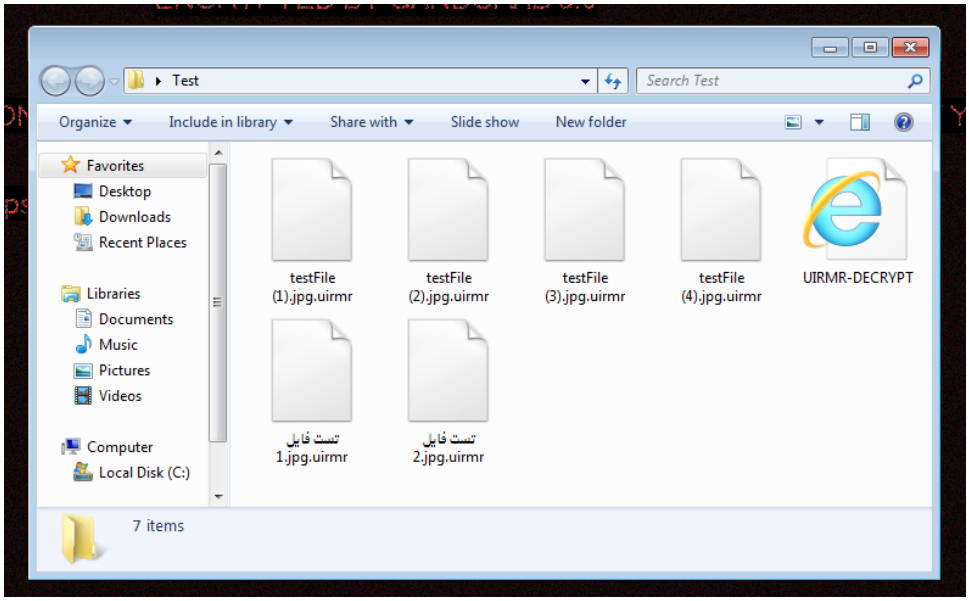
در بررسی و رصد فضای سایبری در زمینه بدافزار، خبر انتشار نسخه پنجم از باج‌افزار GandCrab دیده می‌شود. این نسخه با اضافه کردن پسوند ۵ کاراکتری متشکل از حروف انگلیسی بصورت تصادفی به انتهای هر فایل به کار خود ادامه داده و تمامی فایل‌های شناسایی شده در سیستم را رمزگذاری می‌کند. بعد از اتمام فعالیت باج‌افزار برای فایل‌های دورن یک پوشه، فایل راهنما بصورت -[extension] DECRYPT.html ایجاد کرده و درون پوشه قرار می‌دهد. از تفاوت‌های این نسخه با نسخه‌های قبلی می‌توان به مواردی همچون نوع پسوند اضافه شده، تغییر صفحه دسکتاپ و ارائه راهنما، تغییر پیام نمایش داده شده برای کاربر اشاره کرد. این نسخه با شناسایی اتوماتیک زبان سیستم، اقدام به نمایش فایل راهنما نسبت به آن زبان کرده و در صورتی که زبان سیستم، کشور روسیه باشد، هیچ فعالیتی از خود نشان نداده و متوقف می‌گردد. نحوه انتشار این نسخه بصورت دقیق معلوم نبوده ولی نسخه‌های قبلی این باج‌افزار از طرق ایمیل‌های جعلی، آپدیت جعلی برنامه‌های کاربردی، پروتکل RDP، اکسپلویت کیت Fallout و ... انتشار یافته‌اند. با تحلیل و بررسی کدهای باج‌افزار می‌توان نوع الگوریتم استفاده شده را به الگوریتم Salsa احتمال داد که در نسخه‌های قبلی نیز از آن استفاده شده بود.



شکل ۱ – پیام متنی نشان داده‌شده برای کاربر

نحوه فعالیت بدافزار

باج‌افزار بعد از انتقال و اجرا در سیستم، ابتدا با استفاده از رجیستری سیستم سعی در دریافت زبان مورد استفاده در ویندوز می‌باشد. در بررسی و اجرای باج‌افزار مشاهده می‌گردد که اگر زبان سیستم، زبان روسیه باشد در این صورت فایل باج‌افزار حذف شده و تاثیری در سیستم ندارد ولی در صورتی‌که زبان تشخیص داده شده زبان غیر روسی باشد فعالیت اصلی باج‌افزار شروع می‌گردد. بعد از این مرحله تغییراتی در رجیستری سیستم اتفاق افتاده و مقادیری در رجیستری سیستم ثبت می‌گردد. سپس تمام فایل‌های سیستم را دریافت کرده و آن‌ها را رمز می‌کند. بعد از اتمام کار رمز فایل‌ها، فایل قبلی را حذف کرده و فایل رمزشده جدید را با پسوندی که متشکل از ۵ کاراکتر بصورت تصادفی از حروف انگلیسی می‌باشد، جاگذاری می‌کند. بعد از اتمام رمزگذاری فایل‌های درون پوشه یک فایل متنی را بصورت [extension]-DECRYPT.html را ایجاد و در درون پروشه قرار می‌دهد. بعد از اتمام رمزگذاری فایل‌های سیستم، پس زمینه سیستم را تغییر داده و در آن از کاربر می‌خواهد تا فایل راهنمای ایجاد شده را برای ارتباط با مهاجمان مطالعه کند. سپس شروع به ارسال داده‌هایی برای سرورهای مختلفی می‌کند که در جدول شماره ۶ آدرس سرورهای ارتباطی آورده شده است.



شکل ۲- نمونه‌ای از فایل‌های رمزشده

همچنین در شکل زیر مشاهده می‌گردد که بیشتر آنتی‌ویروس‌های فعال قادر به شناسایی فایل به‌عنوان بدافزار شده‌اند و برای جلوگیری از فعالیت آن می‌توان آنتی‌ویروس خود را بروزرسانی کرده و استفاده کرد.

Ad-Aware	Generic.Ransom.GandCrab4.8CBC6992	ALYac	Generic.Ransom.GandCrab4.8CBC6992
Antiy-AVL	Trojan[Ransom]/Win32.GandCrab	Arcabit	Generic.Ransom.GandCrab4.8CBC6992
Avast	Win32:Malware-gen	AVG	Win32:Malware-gen
Avira	TR/FileCoder.evrob	BitDefender	Generic.Ransom.GandCrab4.8CBC6992
ClamAV	Win.Ransomware.Gandcrab-6667060-0	CrowdStrike Falcon	malicious_confidence_100% (D)
Cybereason	malicious.37561c	Cylance	Unsafe
Cyren	W32/Trojan.UERA-7181	Emsisoft	Generic.Ransom.GandCrab4.8CBC6992 (B)
Endgame	malicious (high confidence)	eScan	Generic.Ransom.GandCrab4.8CBC6992
ESET-NOD32	a variant of Win32/Filecoder.GandCrab.D	F-Secure	Generic.Ransom.GandCrab4.8CBC6992
Fortinet	W32/Filecoder_GandCrab.D!tr	GData	Generic.Ransom.GandCrab4.8CBC6992
Ikarus	Trojan-Ransom.GandCrab	K7AntiVirus	Trojan (00536a1e1)
K7GW	Trojan (00536a1e1)	Kaspersky	HEUR:Trojan.Win32.Generic
Malwarebytes	Ransom.GandCrab	MAX	malware (ai score=100)
McAfee	Ran-GandCrabv4!07FADB006486	McAfee-GW-Edition	BehavesLike.Win32.Generic.ch
Microsoft	Ransom:Win32/GandCrab.MTC!bit	NANO-Antivirus	Trojan.Win32.Filecoder.fifjpt
Palo Alto Networks	generic.ml	Panda	Generic Suspicious
Qihoo-360	HEUR/QVM20.1.13E4.Malware.Gen	Rising	Ransom.GandCrab!8.F355 (CLOUD)
SentinelOne	static engine - malicious	Sophos AV	Mal/Generic-S
Sophos ML	heuristic	Symantec	ML.Attribute.HighConfidence
Tencent	Win32.Trojan.Filecoder.lja	TrendMicro	Ransom_GANDCRAB.THOIBEAH
TrendMicro-HouseCall	Ransom_GANDCRAB.THOIBEAH	VBA32	BScope.TrojanRansom.Cryptor

شکل ۳ - تشخیص فایل در آنتی‌ویروس‌ها

پاکسازی بدافزار از سیستم

برای پاکسازی بدافزار در سیستم در عمل کاری نمی‌توان انجام داد. ولی می‌توان با استفاده از فایل‌های پشتیبان که قبلا از سیستم گرفته‌است، اقدام به بازیابی اطلاعات کرد.

بعد از بازیابی فایل‌ها، سیستم را با استفاده از آنتی‌ویروس بروزشده، اسکن کرده و راهکارهای امنیتی را برای سیستم خود لحاظ می‌کنیم.

راه‌های مراقبت و پیشگیری

برای اینکه سیستم خود را ایمن نگه داریم و از افشای اطلاعات و سواستفاده از آن مراقبت کنیم باید راهکارهای زیر را در نظر بگیریم:

۱- از آنتی‌ویروس‌های قوی و معتبر استفاده کنیم.

بیشتر برنامه‌های آنتی‌ویروس قدرت لازم را برای تشخیص یک فایل بدافزار را ندارند و فقط اسم یک آنتی‌ویروس را بر روی خود دارند. هنگام استفاده از آن‌ها، بعد از تحقیق مختصری در مورد آن‌ها می‌توان یک آنتی‌ویروس قوی و خوبی را انتخاب کرد.

۲- از دانلود و نصب برنامه‌های مشکوک خودداری کنیم.

بیشتر برنامه‌هایی که از طریق تبلیغات یا از طریق کانال‌های دیگر ارائه می‌گردند مخرب بوده و احتمال آسیب رسیدن به سیستم می‌باشد. لذا از دانلود و نصب برنامه‌هایی که مشکوک به‌نظر می‌رسند باید خودداری کرد.

۳- پشتیبان‌گیری مداوم از فایل‌ها و اطلاعات

بیشتر بدافزارها از نوع باج‌افزار می‌باشند و می‌توانند فایل‌ها و اطلاعات موجود بر روی سیستم را رمز کرده و دسترسی به آن‌ها را ناممکن کنند و یا در برخی از بدافزارها امکان حذف یا خرابکاری بر روی اطلاعات وجود دارد. لذا برای درمان بعد از آلوده شدن به بدافزار، به فایل‌های پشتیبان نیاز پیدا می‌کنیم. برای این‌کار بصورت مداوم (هفتگی یا ماهانه) از فایل‌ها و اطلاعات حساس و مورد نیاز فایل پشتیبان ایجاد کرده و آن‌ها را در یک دستگاه دیگر نگهداری کنیم.

۴- عدم بازکردن ایمیل‌های مشکوک

بیشتر حملات باج‌افزاری از طریق اسپم ایمیل‌ها با عناوین گول‌زننده انتشار می‌یابند. لذا باید از باز کردن این نوع از ایمیل‌ها خوودداری کرده و در همان لحظه آن‌ها را حذف کنیم. در این نوع از ایمیل‌ها، در داخل فایل‌های مانند word یا pdf بدافزار قرار داده شده و هنگام اجرای آن‌ها بدافزار اجرا شده و اقدام به نصب و راه‌اندازی خود در سیستم می‌کنند.

آزمایشگاه و مرکز تخصصی آپا دانشگاه محقق اردبیلی

شماره تماس: ۰۴۵ – ۳۱۵۰۵۷۱۸

آدرس اینترنتی: cert.uma.ac.ir

آدرس: اردبیل – خیابان دانشگاه- دانشگاه محقق اردبیلی – دانشکده فنی – مرکز آپا محقق اردبیلی