CSIRT *

مرکز فناوری اطلاعات و ارتباطات

گروه امنیت فضای تبادل اطلاعات

همکار گرامی

در روزهای اخیر انتشار گونه جدیدی از **باج افزار** CTB-Locker در کشورهای مختلف از جمله ایران گزارش شده است.اینگونه جدید نیز مانند بقیه بدافزارهای باجگیر (Ransomware) اقدام به **رمزگذاری** فایلهای کامپیوتر قربانی کرده و از کاربر برای رمزگشایی و برگرداندن فایلها به حالت عادی اخاذی می کند.

این گونه جدید بصورت پیوست ایمیل، در قالب یک فایل ZIP و با یکی از نامهای زیر به کاربر ارسال می گردد:

malformed.zip,plenitude.zip,inquires.zip,simoniac.zip,faltboat.zip,
incurably.zip,payloads.zip,dessiatine.zip

استفاده از موضوعات (Subject) زیر نیز در هرزنامه های ارسالی توسط باجگیر گزارش شده است:

Fax server] +07909 546940]
copy from +07540040842
Message H4H2LC68B7167E4F4
New incoming fax message, S8F8E423F9285C5
Incoming fax from +07843-982843
[Fax server]:+07725-855368
Fax ZC9257943991110
New fax message from +07862-678057

این بدافزار اقدام به رمز کردن فایلها با پسوندهای مختلف از جمله PDF و XLS و txt. ppt. می کند.

* پس از رمز شدن فایلهای مورد نظر بدافزار، یک پنجره مشابه تصویر زیر ظاهر می گردد.

*

* گونه های جدیداین بدافزار با نامهای BackDoor-FCKQ، Downloader-FAMV و Injector-FMZتوسط ضدویروس McAfeeشناسایی می شوند.

* **هشدار** ! گرچه اغلب ضدویروس ها قادر به شناسایی گونه های مختلف CTB-Lockerهستند ولی در صورتیکه بدافزار فرصت داشته و موفق به رمزگذاری فایلهای کامپیوتر آلوده شود، هیچ راهکاری برای رمزگشایی فایلها و برگرداندن آنها به حالت اولیه وجود نخواهد داشت. هیچیک از نرم افزارهای ضدویروس در دنیا قادر به بازگرداندن فایلهای رمز شده نیستند و تنها اقدام به شناسایی و حذف فایلهای مخرب و مرتبط با بدافزار می کنند. تنها راه حل واقعی و عملی برای بازگرداندن فایلها، پرداخت باج است که برای برخی گونه های CTB-Locker مبلغی حدود ۳ میلیون تومان برای هر کامپیوتر هزینه خواهد داشت.

* **اقدامات پیشگیرانه**

* -پرهیز از بازگشایی ایمیل‌ها و پیوست های ناشناس و مشکوک

* -اطمینان از به روز رسانی مستمر و به روز بودن نرم افزار ضد ویروس

* -به روز رسانی سیستم های عامل و نرم افزارهای کاربردی و نصب اصلاحیه های امنیتی آنها