باسمه‌تعالی

گزارش تحلیل باج‌افزار
Crypton

معرفی بدافزار

باج‌افزار Crypton نسخه جدیدی از خود را در ماه مه سال جاری میلادی منتشر کرده که از طریق سرویس‌های آسیب‌پذیر remote desktop خود را به سیستم قربانیان می‌رساند. گزارش‌های ناشی از آلودگی کاربران ایرانی به این باج‌افزار نشان از لزوم آگاهی رسانی و پیشگیری در برابر این باج‌افزار دارد.

مشخصات فایل تحلیل شده

مشخصات فایل تحلیل شده بدین شرح است:

File Name	Rip.exe
MD5	8d30b92d73e16e83d419a7f880db14d4
File Size	91.5 KB
File Type	Executable

سطح تهدید فایل 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 ۴۹ عدد این فایل را به عنوان بدافزار تشخیص داده‌اند.

Ad-Aware	Gen:Trojan.Heur.FU.fGW@a4yATvic	AegisLab	Troj.Ransom.W32.Snocry!c
AhnLab-V3	Trojan/Win32.Snocry.C1923609	ALYac	Trojan.Ransom.Crypton
Antiy-AVL	Trojan[Ransom]/Win32.Snocry	Avast	Win32:Malware-gen
AVG	Win32:Malware-gen	Avira	DR/Delphi.Gen
AVware	Trojan.Win32.Generic!BT	Baidu	Win32.Trojan.WisdomEyes.16070401....
BitDefender	Gen:Variant.Ransom.Nemesis.8	CAT-QuickHeal	Trojan.Cryptolempiz
Comodo	Heur.Packed.Unknown	CrowdStrike Falcon	malicious_confidence_90% (W)
Cyren	W32/Trojan.ZRAW-9362	DrWeb	Trojan.Encoder.11536
Emsisoft	Gen:Variant.Ransom.Nemesis.8 (B)	Endgame	malicious (high confidence)
eScan	Gen:Variant.Ransom.Nemesis.8	ESET-NOD32	a variant of Win32/Filecoder.FP
F-Secure	Gen:Variant.Ransom.Nemesis.8	Fortinet	W32/Crypton.AC!tr.ransom
GData	Win32.Trojan-Ransom.Nemesis.B	Jiangmin	Trojan.Snocry.fg
K7AntiVirus	Trojan (004f15bb1)	K7GW	Trojan (004f15bb1)
Kaspersky	Trojan-Ransom.Win32.Snocry.ddv	Malwarebytes	Ransom.FileLocker
MAX	malware (ai score=99)	McAfee	GenericRXBJ-HZ!8D30B92D73E1
McAfee-GW-Edition	GenericRXBJ-HZ!8D30B92D73E1	Microsoft	Ransom:Win32/CryptoLemPiz.A
NANO-Antivirus	Virus.Win32.Gen.ccmw	Palo Alto Networks	generic.ml
Panda	Trj/CI.A	Qihoo-360	Win32/Trojan.Ransom.cfb
SentinelOne	static engine - malicious	Sophos AV	Troj/Ransom-EMW
Sophos ML	heuristic	Symantec	SMG.Heur!gen
Tencent	Win32.Trojan.Snocry.Ebqm	TrendMicro	Mal_OnCrypt
TrendMicro-HouseCall	Mal_OnCrypt	VBA32	BScope.Trojan-Ransom.Snocry
VIPRE	Trojan.Win32.Generic!BT	ViRobot	Trojan.Win32.Z.Snocry.93696
Webroot	W32.Ransomware.Gen	Zillya	Trojan.Snocry.Win32.577
ZoneAlarm	Trojan-Ransom.Win32.Snocry.ddv	Arcabit	Clean

گزارش تحلیل

بررسی‌های اولیه نشان داد که این بدافزار برای دشوار کردن تحلیل، نام کتابخانه‌ها، توابع و رشته‌های مورد استفاده را مبهم کرده است. برای این کار بدافزار از روش جانشانی ساده‌ای استفاده کرده است. این امر باعث می‌شود در زمان اجرای بدافزار، این رشته‌ها کدگشایی و کتابخانه‌های مورد استفاده بارگذاری شوند. بدافزار پس

از اجرا شدن، در اولین گام، زبان مورد استفاده سیستم را بررسی می‌کند و در صورتی که یکی از زبان‌های روسی، اوکراینی و قرافستانی باشد به فعالیت خود خاتمه می‌دهد. همچنین بدافزار اجرا شدن در دیباگر و ماشین های مجازی را تشخیص می‌دهد و در صورت تشخیص دادن اجرا در چنین محیط‌هایی به فعالیت خود خاتمه می‌دهد.

کسب ماندگاری در سیستم

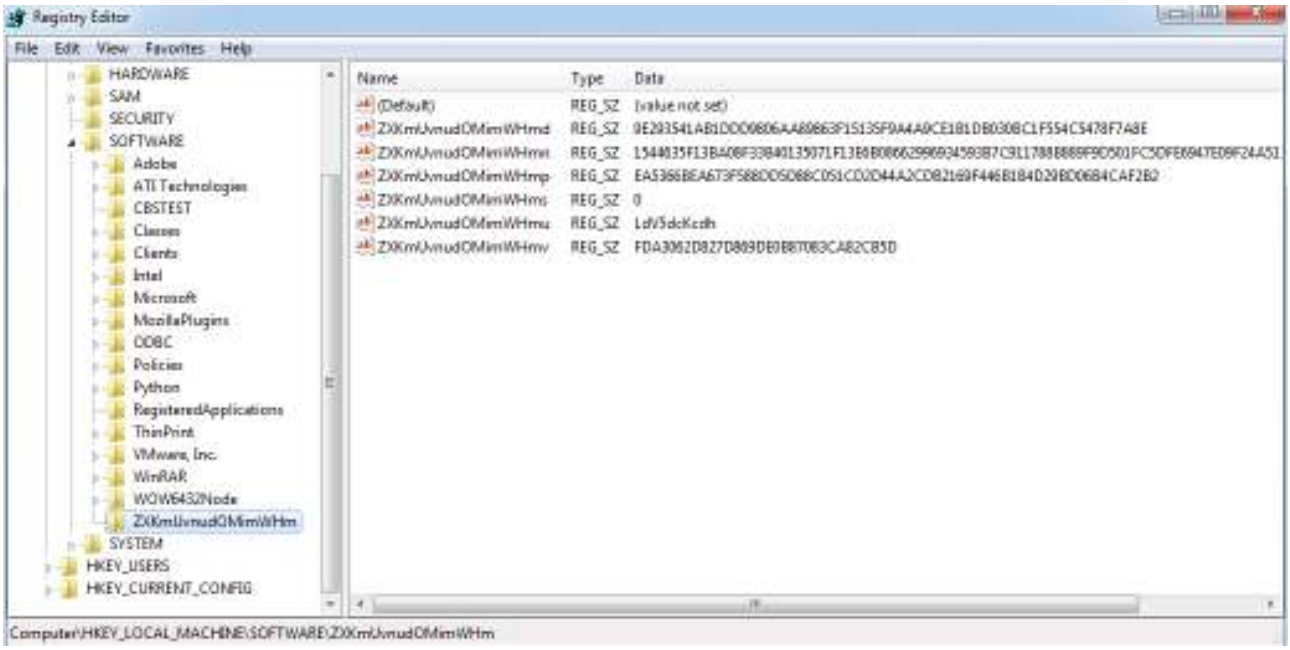
برای کسب ماندگاری در سیستم، بدافزار فایل اجرایی خود را به عنوان مقداری برای کلید رجیستری HKEY_CURRENT_USER\Software\Microsoft\CurrentVersion\Run\ZXKmUvnudOMimWHm تنظیم می‌کند.

حذف فایل‌های پشتیبان

باج‌افزار پس از بررسی اجرا شدن در بالاترین سطح و اتصال به اینترنت، با استفاده از تابع SRRemoveRestorePoint اقدام به حذف فایل‌های بکاپ سیستم می‌نماید تا بازیابی فایل‌های رمز شده غیر ممکن باشد.

فراهم کردن مقدمات رمزگذاری

در ادامه باج‌افزار با استفاده از اطلاعاتی شامل نام کاربری، نام رایانه و شماره سریال درایو اصلی سیستم، شناسه‌ای یکتا برای قربانی ایجاد می‌کند. این شناسه برای متمایز کردن قربانی از سایر قربانیان استفاده می‌شود. بدافزار برای نگهداری اطلاعات شناسه قربانی و اطلاعات مورد استفاده برای رمزگذاری داده‌ها کلیدی در مسیر HKLM\SOFTWARE با نام ZXKmUvnudOMimWHm ایجاد می‌کند و اطلاعات مورد نظر خود را که با استفاده از روش جانشانی کدگذاری کرده است به عنوان مقادیری در درایه‌های ZXKmUvnudOMimWHmd، ZXKmUvnudOMimWHmn، ZXKmUvnudOMimWHmp، ZXKmUvnudOMimWHms، ZXKmUvnudOMimWHmu و ZXKmUvnudOMimWHmv قرار می‌دهد. نام درایه‌ها از ترکیب ZXKmUvnudOMimWHm و حروف d، n، p، s، u و v ساخته شده است. شکل زیر نمونه مقادیر این کلید رجیستری را نمایش می‌دهد. به عنوان نمونه کدگذاری شده شناسه قربانی در ZXKmUvnudOMimWHmu قرار گرفته است.



ارسال اطلاعات برای سرور راه دور

در ادامه بدافزار جزئیات دیگری از سیستم قربانی شامل نام رایانه، سیستم عامل مورد استفاده، نوع معماری سیستم و زبان مورد استفاده در سیستم را به‌دست می‌آورد و با استفاده از این اطلاعات رشته‌ای به فرمت زیر تولید می‌کند.

Report||RansomID||HEX(RansomID_)<p value>hex(_)<v value>hex(_)<n value>hex(_)<d value>
Computername||os type||architext(x32 or x64)||language(US)

پس از رمز کردن این رشته، آن را به صورتی مشابه

Data=
91CFA105698128CD7AED0287B311E68546194AA16EB3895F78C0C9C9E3881EF5EC3FCE
186F733ECBC197C9DE4A3318200695F10CB01A975C966AE89868F41E3DBB463504FF45
CB596F2D75C5A1ED78F359C696C15CABBCC45C2DDA14F8F70A1A4A00A4054E3CECD
F22D8A2B6E980EB153806FFF5

در آورده و با استفاده از متد POST پروتکل HTTP برای سرور خود در آدرس زیر ارسال می‌نماید:

http://auth-rambler.com/krya18/index_shell.php

عملیات رمزگذاری اطلاعات

در صورتی که باج‌افزار پس از ارسال اطلاعات مذکور سمت سرور، پاسخ RESULTOK را از سرور دریافت کند شروع به رمزگذاری اطلاعات می‌نماید. برای این کار در ابتدا شروع به پویش منابع به اشتراک‌گذاری شده در شبکه و سپس درایوهای فیزیکی سیستم و فایل‌های موجود در آن‌ها می‌کند و در هر پوشه، فایل راهنمای رمزگشایی را کپی می‌کند.

Crypton برای رمز کردن اطلاعات از الگوریتم AES با کلید ۱۲۸ بیتی استفاده می‌کند. باج‌افزار تمامی فایل‌های سیستم به جز فایل‌هایی که در مسیر نام خود مقادیر زیر را داشته باشند رمز می‌کند:

\windows\;\programdata\;nvidia;intel;.sys;.dll;.lnk;boot.ini;ntdetect.com;bootfont.bin;ntldr;boot mgr;bootnxt;bootsect.bak;ntuser.dat;pdoxusrs.net;internet explorer;mozilla firefox;opera;google

پس از رمزگذاری تمامی فایل‌های موجود در سیستم، crypton آمار تعداد فایل‌های رمز شده را برای سرور راه دور خود ارسال می‌کند. این آمار به صورت

"||statistic||3791706078||WIN-94KJT5VS6N9||0||5785||1553"

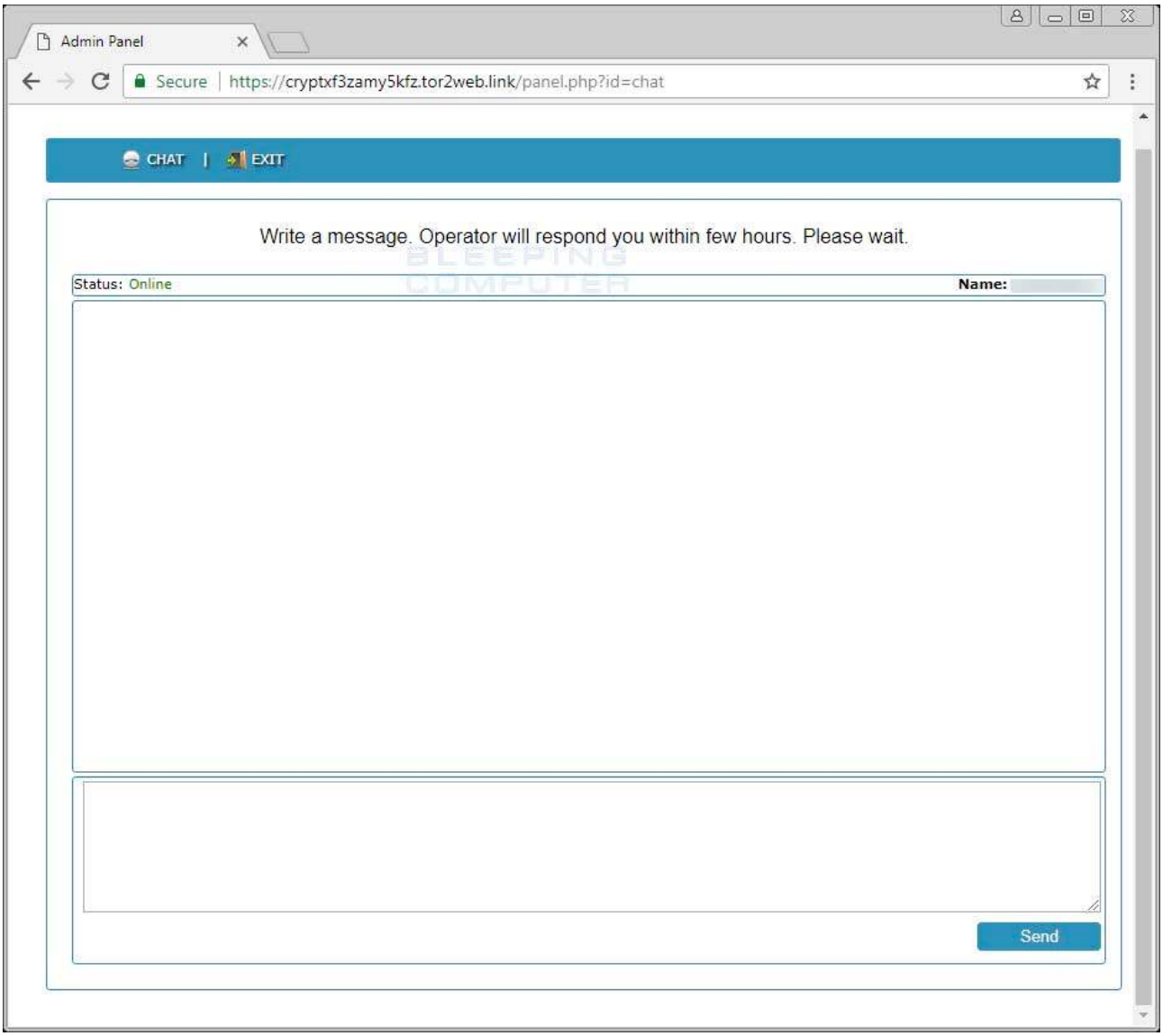
است که در آن شناسه قربانی، نام رایانه و تعداد فایل‌های رمز شده قرار گرفته است. این رشته پیش از ارسال شدن کدگذاری می‌شود و به صورت data=... ارسال می‌شود.

تغییرات سیستم پس از پایان رمزنگاری

در نهایت، بدافزار کلید رجیستری که برای ماندگاری در سیستم ایجاد کرده بود و کلیدهای رجیستری که مقادیر کلیدهای رمزنگاری در آنها قرارداده شده بود را حذف می‌کند. همچنین مقدار کلید رجیستری ZXKmUvnudOMimWHms را که در ابتدا و پیش از رمزگذاری اطلاعات صفر بود به ۱ افزایش می‌دهد. در واقع این کلید شمارنده تعداد مرتبه‌های رمزگذاری اطلاعات سیستم است. سپس تصویر زیر از منابع باج‌افزار استخراج می‌شود. Crypton این تصویر را به عنوان تصویر صفحه نمایش سیستم تنظیم می‌کند.

بدافزار فایل راهنمای رمزگشایی را از منابع خود استخراج کرده و آن را با یکی از مرورگرهای مورد استفاده کاربر نمایش می‌دهد.

در این فایل لینک‌هایی برای ارتباط با مهاجم اصلی و دریافت دستورالعمل رمزگشایی قرار داده شده است.



در نهایت بدافزار با ایجاد اسکرپیتی هم‌نام خود، فایل اجرایی خود و فایل اسکریپت را از روی سیستم حذف می‌کند و به اجرای خود خاتمه می‌دهد.