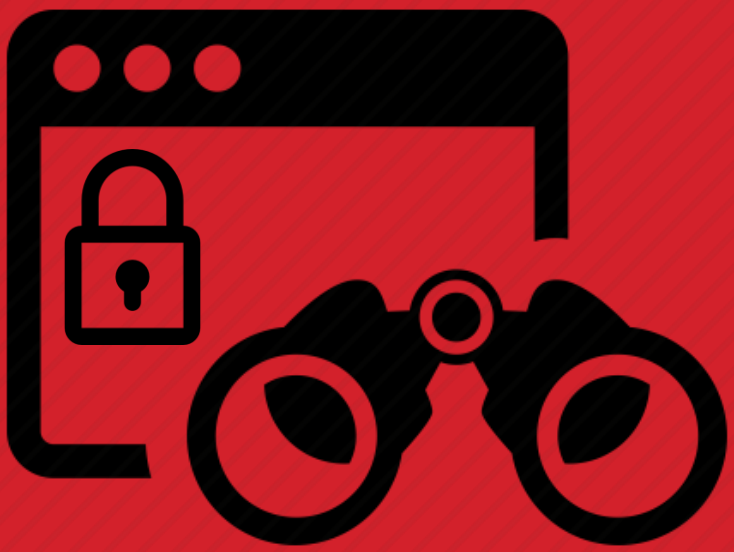
بـررسـی و تـحـلـیـل بـاج‌افـزار

# WALLET



شبکه گستر
شـرکت مهندسی شـبکه گسـتر

عنوان سند: بررسی و تحلیل باج‌افزار Wallet
شناسه سند: SPT-A-0131-00
تهیه‌کننده: گروه تحقیق و توسعه، شرکت مهندسی شبکه گستر
تاریخ آخرین بازنگری: ۱۷ اسفند ۱۳۹۵ | شرح آخرین بازنگری: -

شبکه گستر

نخستین نسخه از باج‌افزار Wallet که با نام CrySis نیز شناخته می‌شود در زمستان سال ۹۴ شناسایی شد. از آن زمان تا کنون این باج‌افزار از راه‌های مختلفی ایستگاه‌های کاری و سرورها را در نقاط مختلف جهان از جمله ایران هدف قرار داده است.

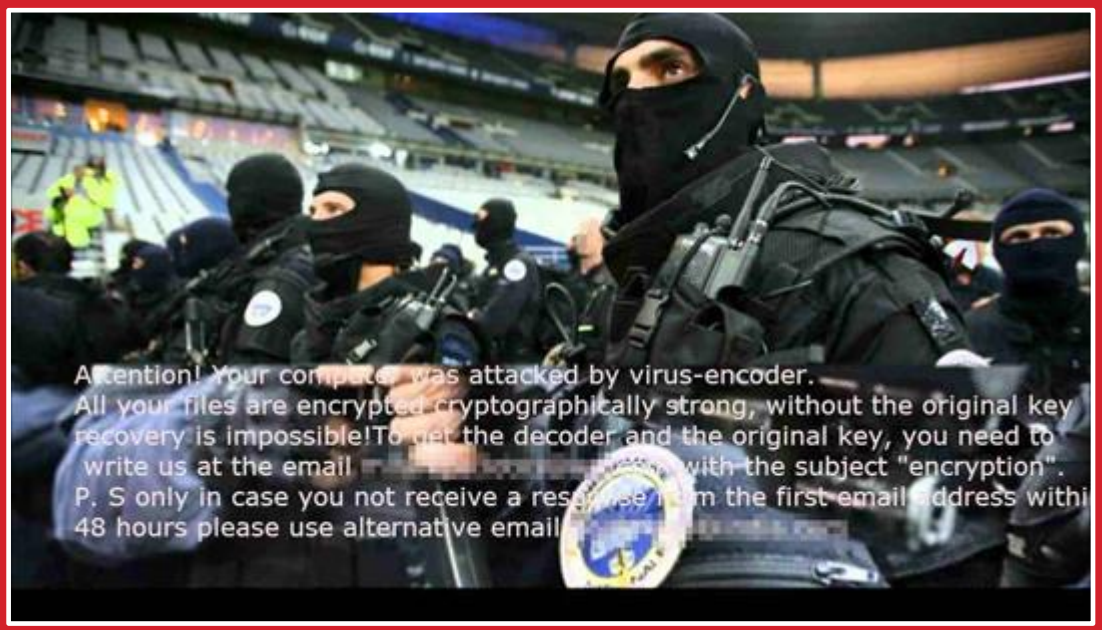
یکی از روش‌های مورد استفاده صاحبان باج‌افزار Wallet به‌منظور گسترش آلودگی، اتصال به دستگاه‌هایی با گذرواژه ضعیف از طریق پودمان RDP است.

Wallet باج‌افزاری رمزگذار است که با بکارگیری الگوریتم‌های RSA و AES و با استفاده از یک کلید طولانی دامنه گسترده‌ای از فایل‌های کاربر را رمزنگاری می‌کند.

در آذر ماه ۹۵، در یک اقدام عجیب کاربری اقدام به انتشار کلیدهای رمزگشایی این باج‌افزار در یک تالار گفتگوی اینترنتی کرد. اقدامی که منجر به ساخت ابزار رمزگشایی برای نجات قربانیان این باج‌افزار توسط چند شرکت ضدویروس شد. اما نه تنها روند کار صاحبان این باج‌افزار متوقف نشد که نسخه‌هایی جدیدتر از آن عرضه و کاربران بیشتری هدف آن قرار گرفتند.

Wallet یکی از بازیگران اصلی در صنعت باج‌گیری اینترنتی در طی یک سال گذشته بوده و گسترش آلودگی‌های آن نشان می‌دهد صاحبان این باج‌افزار حداقل به این زودی‌ها قصد کنار گذاشتن آن را ندارند.

در این گزارش، ساختار و روش‌های انتشار باج‌افزار Wallet مورد بررسی و تحلیل قرار گرفته است.




شکل ۱: نمونه‌ای از اطلاعیه باج‌گیری Wallet

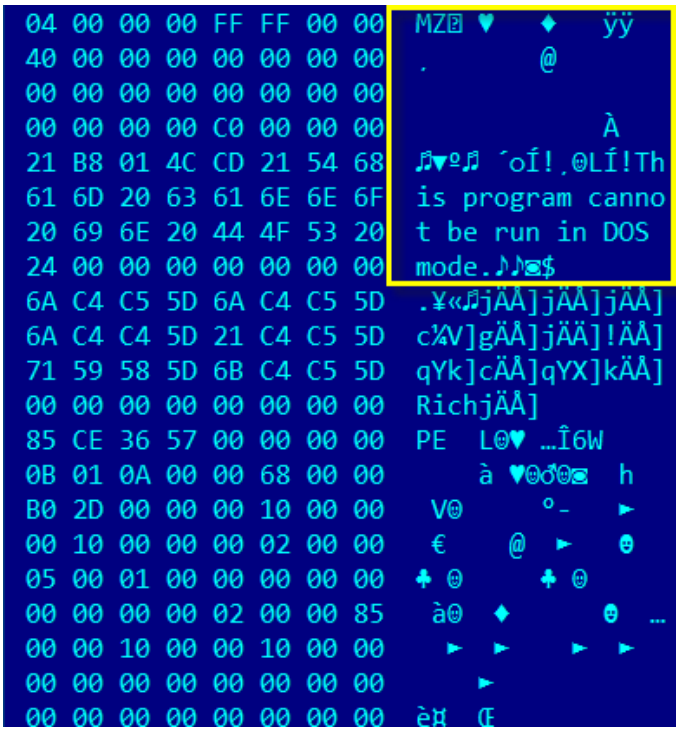
Wallet باج‌افزاری رمزگذار[۱] است که همانطور که از نام آن پیداست با انجام رمزنگاری[۲]، دسترسی به فایل‌های کاربر را محدود ساخته و برای دسترسی مجدد، از او اخاذی می‌کند.

باج‌افزار Wallet با استفاده از الگوریتم‌های RSA و AES و با بکارگیری یک کلید رمزنگاری[۳] طولانی اقدام به رمزگذاری فایل‌های کاربر می‌کند. این بدان معناست که رمزگشایی[۴] فایل‌های رمز شده بدون در اختیار داشتن کلید عملاً غیرممکن است.

این باج‌افزار زمانی به شهرت رسید که انتشار باج‌افزار TeslaCrypt – به دلیل عرضه ابزار رمزگشایی برای آن – متوقف شد و صاحبان Wallet به‌سرعت موفق به پر کردن جای خالی آن شدند.

## خرابکاری بر روی دستگاه

فایل مخرب این باج‌افزار فایلی اجرایی است که توسط هیچ مکانیزم مبهم‌سازی[۵] نظیر Packer محافظت نمی‌شود.



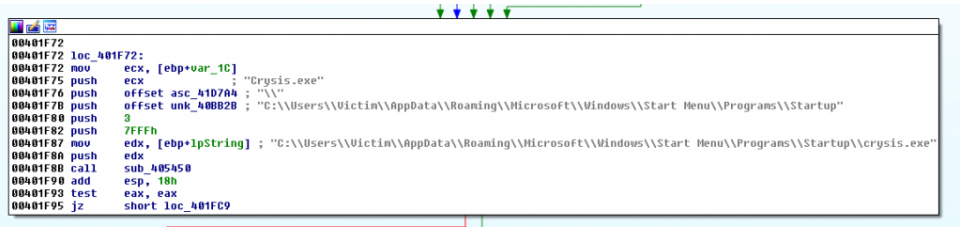

شکل ۲: عدم استفاده از Packer در فایل مخرب اجرایی باج‌افزار

این باج‌افزار، به‌محض اجرا شدن، نسخه‌هایی از خود را در مسیرهای زیر بر روی دستگاه قربانی کپی می‌کند:

- `%localappdata%\Microsoft\Windows\Start Menu\Programs\Startup\%originalmalwarefilename%.exe`
- `%localappdata%\%originalmalwarefilename%.exe`
- `%windir%\system32\%originalmalwarefilename%.exe`

---

۱ Crypto Ransomware
۲ Encryption
۳ Encryption Key
۴ Decryption
۵ Obfuscation




شکل ۳: فرامین مربوط به کپی نسخه‌ای از باج‌افزار

Wallet، علاوه بر ایجاد نسخه‌ای از خود در پوشه Startup که سبب اجرای خودکار آن در هر بار راه‌اندازی شدن سیستم عامل می‌شود، کلیدهای زیر را نیز در محضرخانه[۶] با همان هدف ایجاد می‌کند.

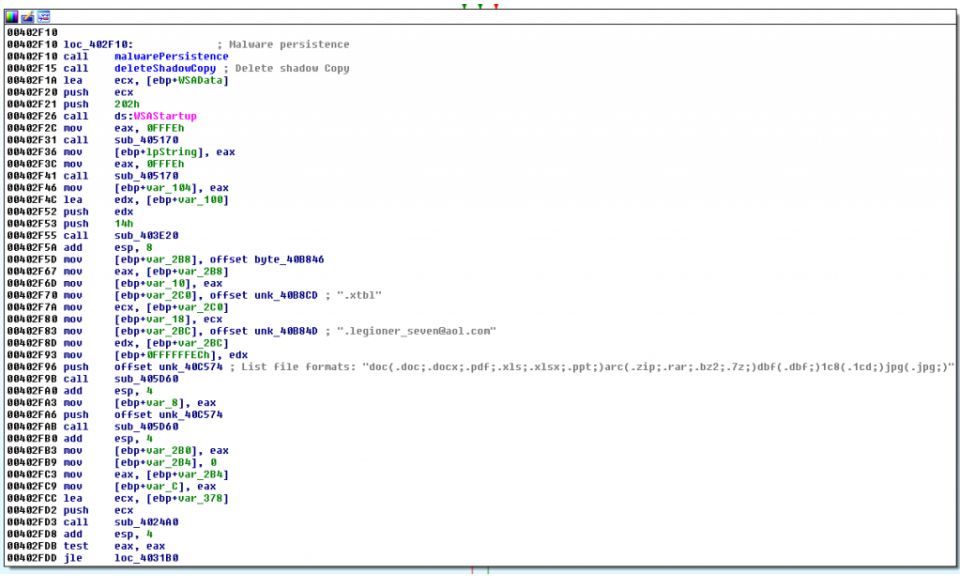
- `[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]`
  `"%originalmalwarefilename%" = "%installpath%\%originalmalwarefilename%.exe"`
- `[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]`
  `"%originalmalwarefilename%" = "%installpath%\%originalmalwarefilename%.exe"`

در ادامه فایل‌های دستگاه، حافظه‌های حذف‌شدنی[۷] متصل به آن و پوشه‌های اشتراکی[۸] برای یافتن فایل‌هایی با پسوندهای هدف قرار گرفته شده مورد جستجو قرار می‌گیرند. Wallet بیش از ۱۸۵ پسوند فایل از جمله فایل‌های با پسوند EXE را هدف قرار می‌دهد.

توضیح اینکه باج‌افزار Wallet به فایل‌های رمز شده پسوندی حاوی چهار یا شش نویسه را الصاق کرده و نام آنها را بر اساس الگوی زیر تغییر می‌دهد.

- `[filename].id-[id].[email_address].[Four/Six-Character]`

ایمیل و پسوند استفاده شده در این باج‌افزار در نسخه‌های مختلف آن متفاوت بوده است. wallet و xtbl از جمله پسوندهای معروف استفاده شده توسط این باج‌افزار هستند.




شکل ۴: بخشی از فهرست پسوندهای هدف قرار گرفته شده و الگوی نامگذاری در Wallet

[۶] Registry
[۷] Removable Storage
[۸] Shared Folder

Wallet از رمزگذاری فایل‌های موجود در پوشه Windows و فایل‌های زیر صرف‌نظر می‌کند:

- boot.ini
- explorer.exe
- svchost.exe
- %originalmalwarefilename%.exe

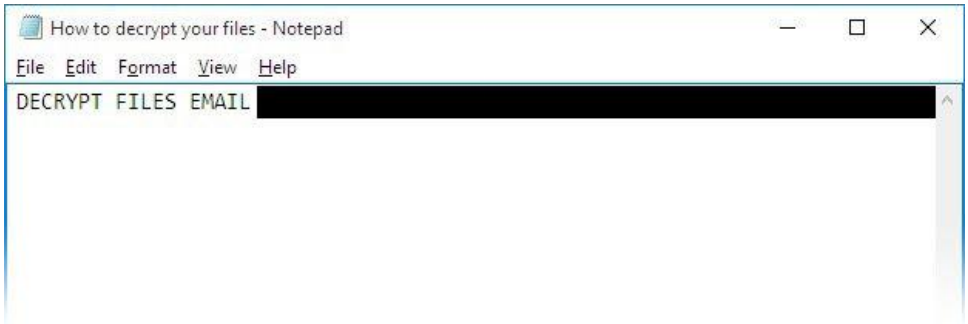
Wallet نسخه‌های Windows Shadow Volume را نیز با اجرای فرامین زیر از روی دستگاه حذف می‌کند.

```
mode con cp select=1251
vssadmin delete shadows /all /quiet
Exit
```

```
00402C50
00402C50 PipeAttributes= _SECURITY_ATTRIBUTES ptr -88h
00402C50 var_7C= dword ptr -7Ch
00402C50 hReadPipe= dword ptr -78h
00402C50 hWritePipe= dword ptr -74h
00402C50 lpString= dword ptr -70h
00402C50 NumberOfBytesWritten= dword ptr -6Ch
00402C50 StartupInfo= _STARTUPINFOW ptr -68h
00402C50 lpApplicationName= dword ptr -1Ch
00402C50 ProcessInformation= _PROCESS_INFORMATION ptr -18h
00402C50 hObject= dword ptr -8
00402C50 var_4= dword ptr -4
00402C50
00402C50 push    ebp
00402C51 mov     ebp, esp
00402C53 sub     esp, 88h
00402C59 mov     [ebp+lpString], offset unk_40C132 ; "mode con cp select=1251\nvssadmin delete shadows /all /quiet\nExit\n"
00402C60 mov     [ebp+var_7C], offset unk_40BA17 ; "%comspec%"
00402C67 mov     eax, 1FFFCh
00402C6C call    sub_405170
00402C71 mov     [ebp+lpApplicationName], eax ; "C:\Windows\System32\cmd.exe"
00402C74 push    44h
00402C76 push    0
00402C78 lea     eax, [ebp+StartupInfo]
00402C7B push    eax
00402C7C call    sub_4052C0
00402C81 add     esp, 0Ch
00402C84 push    0Ch
00402C86 push    0
00402C88 lea     ecx, [ebp+PipeAttributes]
00402C8E push    ecx
00402C8F call    sub_4052C0
00402C94 add     esp, 0Ch
00402C97 mov     [ebp+PipeAttributes.bInheritHandle], 1
```

شکل ۵: فرامین حذف نسخه‌های Windows Shadow Volume از روی دستگاه آلوده

اطلاعیه باج‌گیری[۹] Wallet نیز در نسخه‌های مختلف آن متفاوت بوده است. تصاویر ۱، ۶ و ۷ نمونه‌هایی از اطلاعیه‌ها را نشان می‌دهند.




شکل ۶: نمونه‌ای از اطلاعیه باج‌گیری Wallet با نام How to decrypt your files.txt در پوشه Desktop

[۹] Ransom Note


شکل ۷: نمونه‌ای از اطلاعیه باج‌گیری Wallet

```
00402FFA push    offset asc_41D80C ; ";"
00402FFF push    offset unk_40BD47 ; "How to decrypt your files.txt"
00403004 push    offset asc_41D810 ; ";"
00403009 push    offset unk_40BC47 ; "How decrypt your files.jpg"
0040300E push    offset asc_41D814 ; ";"
00403013 push    offset unk_40CD74 ; "boot.ini;boot.bin;ntldr;ntdetect.com;io.sys;"
00403018 push    6
0040301A push    7FFFh
0040301F mov     eax, [ebp+lpString]
00403025 push    eax
00403026 call    sub_405450
0040302B add     esp, 24h
0040302E mov     ecx, [ebp+lpString]
00403034 push    ecx             ; lpString
00403035 call    ds:lstrlenW
0040303B mov     edx, [ebp+lpString]
00403041 lea     eax, [edx+eax*2]
00403044 mov     [ebp+var_D4], eax
0040304A push    1
0040304C mov     ecx, [ebp+var_104]
00403052 push    ecx
00403053 call    sub_406180
00403058 add     esp, 8
0040305B test    eax, eax
0040305D jz      short loc_403094
```

شکل ۸: فرامین مربوط به ایجاد اطلاعیه باج‌گیری Wallet

Wallet اطلاعاتی نظیر نام و شناسه منحصربه‌فرد دستگاه را از طریق پودمان HTTP به سرور فرماندهی[۱۰] ارسال می‌کند. سرورهای فرماندهی این باج‌افزار سایت‌های هک شده‌ای هستند که عمدتاً توسط نسخه‌ای آسیب‌پذیر از سامانه مدیریت محتوای WordPress میزبانی می‌شوند.

[۱۰] Command and Control – C&C – C2

## روش انتشار

نخستین نسخه‌های این باج‌افزار از طریق هرزنامه‌ها[11] با فایل پیوست دو پسوندی[12] منتشر می‌شدند. با توجه به عدم نمایش پسوندهای شناخته شده به‌صورت پیش فرض در سیستم عامل Windows، بسیاری از دریافت‌کنندگان هرزنامه‌ها، فایل پیوست را نه اجرایی، که یک فایل عادی تصور می‌کردند.

برخی از هرزنامه‌ها نیز حاوی لینکی یا لینک‌هایی به سایت‌های هک شده‌ای بودند که با کلیک کاربر بر روی هر یک از آنها، کاربر به فایل مخرب هدایت می‌شد.

شرکت ESET نیز در گزارشی به اشتراک‌گذاری فایل‌های مخرب این باج‌افزار بر روی اینترنت در قالب فایل‌های نصب برنامه‌هایی نظیر WinRAR، Microsoft Excel و iExplorer اشاره کرده است.

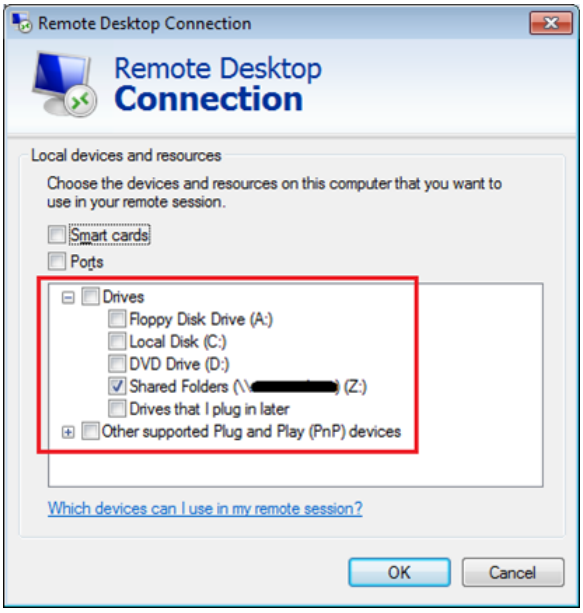
اما یکی از روش‌های خاص – و البته نه منحصربه‌فرد – مورد استفاده صاحبان Wallet جهت انتشار این باج‌افزار رخنه نمودن به دستگاه‌ها از طریق پودمان RDP[13] است.

در این روش مهاجمان با شناسایی دستگاه‌هایی با نشانی IP عمومی بر روی اینترنت، باز بودن پودمان RDP را بررسی کرده و سپس با اجرای حملات موسوم به "جستجوی فراگیر"[14] اقدام به اتصال به آنها می‌کنند.

ابزارهای استفاده شده در حملات جستجوی فراگیر تمامی حالات ممکن را تا رسیدن به جواب بررسی می‌کنند. طبیعی است که در صورت استفاده از گذرواژه‌های پیچیده[15] با طول مناسب، بررسی تمامی حالات ممکن، به سال‌ها زمان نیاز دارد. بنابراین این مهاجمان نیز جستجوی خود را محدود به گذرواژه‌هایی با طول کوتاه می‌کنند. با این امید که گذرواژه دستگاه، ساده و کوتاه باشد.

در صورت موفقیت در کشف گذرواژه، مهاجمان به دستگاه متصل شده و ضمن آلوده کردن آن، باج‌افزار را در سطح شبکه منتشر می‌کنند.

در این روش انتقال فایل مخرب به دستگاه قربانی، با ایجاد پوشه‌ای اشتراکی بر روی دستگاه مهاجم و فعال کردن آن در زمان اتصال انجام می‌شود.

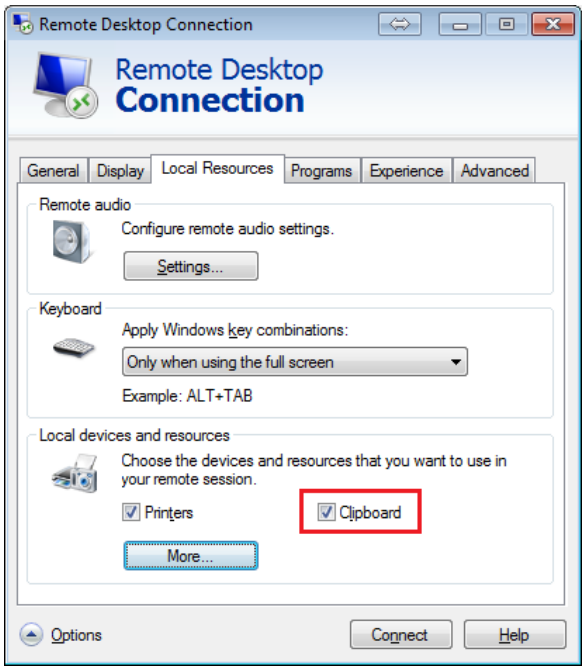



شکل ۹: اتصال به دستگاه قربانی و انتقال فایل مخرب به آن از طریق پوشه اشتراکی ایجاد شده بر روی دستگاه مهاجم

---

[11] Spam
[12] Double Extension
[13] Remote Desktop Protocol
[14] Brute Force
[15] Complex Password

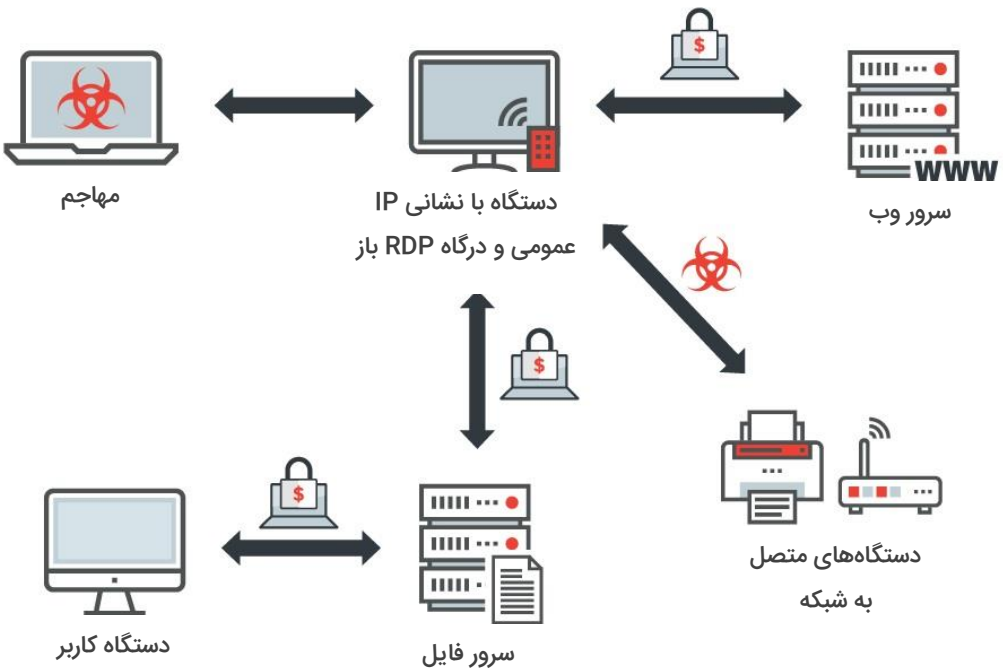
در برخی نمونه‌ها نیز انتقال فایل مخرب با فعال کردن بخش Clipboard انجام می‌شود.




شکل ۱۰: اتصال به دستگاه قربانی و انتقال فایل مخرب به آن از طریق Clipboard

نمونه‌هایی نیز مشاهده شده است که در آنها مهاجمان پس از اتصال به هر یک از دستگاه‌ها نسخه‌ای متفاوت از باج‌افزار را نصب کرده‌اند.

شکل ۱۱ نحوه انتشار باج‌افزار Wallet از طریق پودمان RDP را نمایش می‌دهد.




شکل ۱۱: نحوه انتشار باج‌افزار Wallet از طریق پودمان RDP

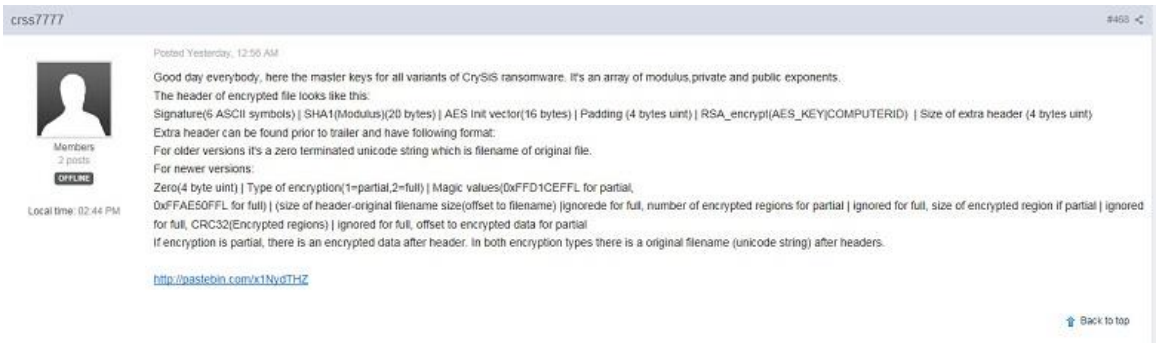
در اسفند ماه ۹۵، نیز مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه‌ای (ماهر)، اعلام کرد که گزارش‌های متعددی از حمله باج‌افزارها از طریق پودمان RDP به سرورهایی با سیستم عامل Windows در کشور به این مرکز واصل شده است.

رخنه به دستگاه از طریق پودمان RDP موضوع جدیدی در حملات سایبری نیست. حتی در دنیای این نوع بدافزارهای مخرب نیز پیش از Wallet، باج‌افزارهای LowLevel، DMA Locker، Apocalypse، Smrss32، Bucbi، Aura/BandarChor، ACCDFISA و Globe از این روش جهت انتشار بهره برده‌اند.

> در اسفند ماه، مرکز ماهر اعلام کرد که گزارش‌های متعددی از حمله باج‌افزارها از طریق پودمان RDP به سرورهایی با سیستم عامل Windows در کشور به این مرکز واصل شده است.

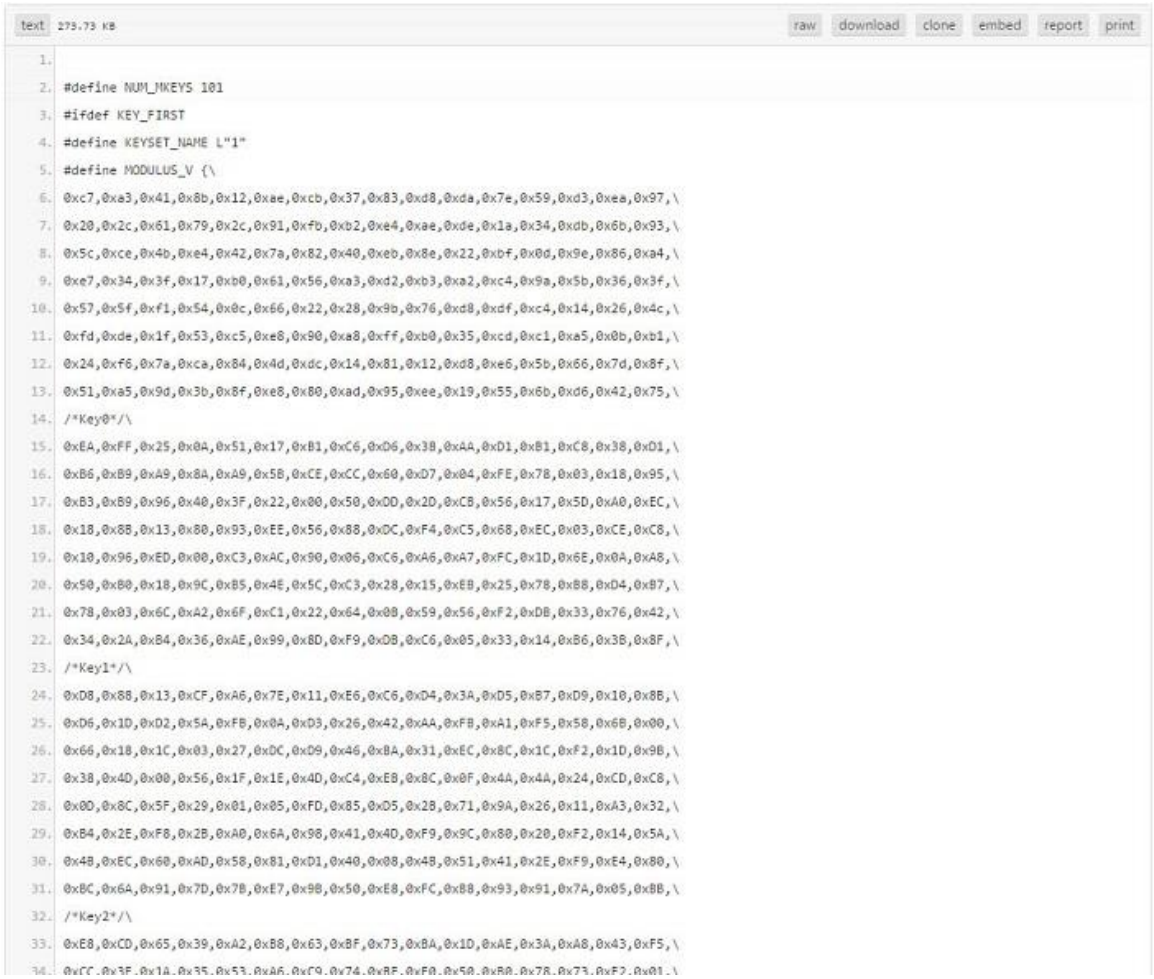
## ابزارهای رمزگشایی

در آذر ماه ۹۵، در یک اقدام عجیب کاربری با شناسه crss7777 کلیدهای رمزگشایی باج‌افزار Wallet را در تالار گفتگوی[۱۶] CrySiS Support Topic سایت اینترنتی Bleeping Computer در قالب لینکی به یک فایل سرآیند[۱۷] زبان برنامه‌نویسی C به اشتراک گذاشت.




شکل ۱۲: انتشار کلیدهای رمزگشایی Wallet در یک تالار گفتگوی اینترنتی

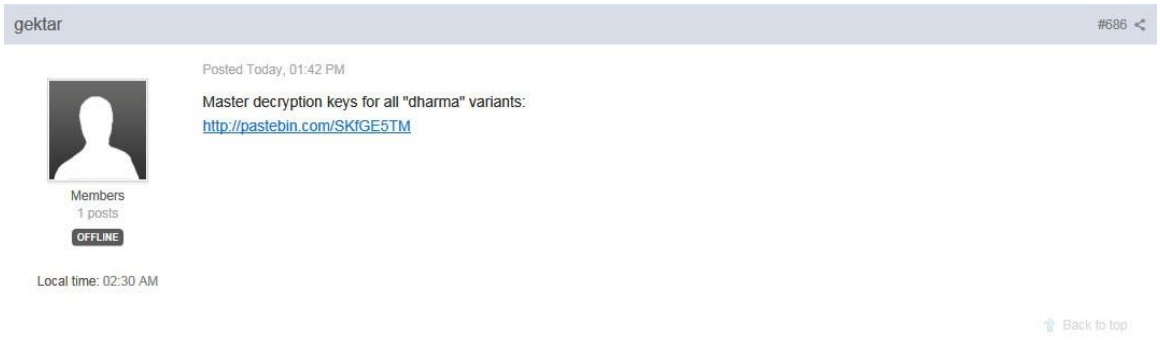
[۱۶] Forum
[۱۷] Header



```
#define NUM_MKEYS 101
#ifdef KEY_FIRST
#define KEYSET_NAME L"1"
#define MODULUS_V {\
0xc7,0xa3,0x41,0x8b,0x12,0xae,0xcb,0x37,0x83,0xd8,0xda,0x7e,0x59,0xd3,0xea,0x97,\
0x20,0x2c,0x61,0x79,0x2c,0x91,0xfb,0xb2,0xe4,0xae,0xde,0x1a,0x34,0xdb,0x6b,0x93,\
0x5c,0xce,0x4b,0xe4,0x42,0x7a,0x82,0x40,0xeb,0x8e,0x22,0xbf,0x0d,0x9e,0x86,0xa4,\
0xe7,0x34,0x3f,0x17,0xb0,0x61,0x56,0xa3,0xd2,0xb3,0xa2,0xc4,0x9a,0x5b,0x36,0x3f,\
0x57,0x5f,0xf1,0x54,0x0c,0x66,0x22,0x28,0x9b,0x76,0xd8,0xdf,0xc4,0x14,0x26,0x4c,\
0xfd,0xde,0x1f,0x53,0xc5,0xe8,0x90,0xa8,0xff,0xb0,0x35,0xcd,0xc1,0xa5,0x0b,0xb1,\
0x24,0xf6,0x7a,0xca,0x84,0x4d,0xdc,0x14,0x81,0x12,0xd8,0xe6,0x5b,0x66,0x7d,0x8f,\
0x51,0xa5,0x9d,0x3b,0x8f,0xe8,0x80,0xad,0x95,0xee,0x19,0x55,0x6b,0xd6,0x42,0x75,\
/*Key0*/\
0xEA,0xFF,0x25,0x0A,0x51,0x17,0xB1,0xC6,0xD6,0x38,0xAA,0xD1,0xB1,0xC8,0x38,0xD1,\
0xB6,0xB9,0xA9,0x8A,0xA9,0x58,0xCE,0xCC,0x60,0xD7,0x04,0xFE,0x78,0x03,0x18,0x95,\
0xB3,0xB9,0x96,0x40,0x3F,0x22,0x00,0x50,0xDD,0x2D,0xCB,0x56,0x17,0x5D,0xA0,0xEC,\
0x18,0x88,0x13,0x80,0x93,0xEE,0x56,0x88,0xDC,0xF4,0xC5,0x68,0xEC,0x03,0xCE,0xC8,\
0x10,0x96,0xED,0x00,0xC3,0xAC,0x90,0x06,0xC6,0xA6,0xA7,0xFC,0x1D,0x6E,0x0A,0xA8,\
0x50,0xB0,0x18,0x9C,0xB5,0x4E,0x5C,0xC3,0x28,0x15,0xEB,0x25,0x78,0xB8,0xD4,0xB7,\
0x78,0x03,0x6C,0xA2,0x6F,0xC1,0x22,0x64,0x08,0x59,0x56,0xF2,0xDB,0x33,0x76,0x42,\
0x34,0x2A,0xB4,0x36,0xAE,0x99,0x8D,0xF9,0xDB,0xC6,0x05,0x33,0x14,0xB6,0x3B,0x8F,\
/*Key1*/\
0xD8,0x88,0x13,0xCF,0xA6,0x7E,0x11,0xE6,0xC6,0xD4,0x3A,0xD5,0xB7,0xD9,0x10,0x8B,\
0xD6,0x1D,0xD2,0x5A,0xFB,0x0A,0xD3,0x26,0x42,0xAA,0xFB,0xA1,0xF5,0x58,0x6B,0x00,\
0x66,0x18,0x1C,0x03,0x27,0xDC,0xD9,0x46,0xBA,0x31,0xEC,0x8C,0x1C,0xF2,0x1D,0x9B,\
0x38,0x4D,0x00,0x56,0x1F,0x1E,0x4D,0xC4,0xE8,0x8C,0x0F,0x4A,0x4A,0x24,0xCD,0xC8,\
0x0D,0x8C,0x5F,0x29,0x01,0x05,0xFD,0x85,0xD5,0x28,0x71,0x9A,0x26,0x11,0xA3,0x32,\
0xB4,0x2E,0xF8,0x2B,0xA0,0x6A,0x98,0x41,0x4D,0xF9,0x9C,0x80,0x20,0xF2,0x14,0x5A,\
0x48,0xEC,0x60,0xAD,0x58,0x81,0xD1,0x40,0x08,0x4B,0x51,0x41,0x2E,0xF9,0xE4,0x80,\
0xBC,0x6A,0x91,0x7D,0x7B,0xE7,0x98,0x50,0xE8,0xFC,0xB8,0x93,0x91,0x7A,0x05,0xBB,\
/*Key2*/\
0xE8,0xCD,0x65,0x39,0xA2,0xB8,0x63,0xBF,0x73,0xBA,0x1D,0xAE,0x3A,0xA8,0x43,0xF5,\
0xCC,0x3F,0x1A,0x35,0x53,0xA6,0xC9,0x74,0xBF,0xF0,0x50,0xB0,0x78,0x73,0xF2,0x01,\
```

شکل ۱۳: کلیدهای رمزگشایی Wallet

در اسفند ماه ۹۵، نیز در اقدامی مشابه کاربری با شناسه gektar کلیدهای رمزگشایی باج‌افزار Dharma – یکی از باج‌افزارهای مبتنی بر Wallet - را در تالار گفتگوی Dharma Ransomware Support Topic همان سایت اینترنتی به اشتراک گذاشت.




شکل ۱۴: انتشار کلیدهای رمزگشایی Dharma در یک تالار گفتگوی اینترنتی

اطلاعاتی در خصوص هویت واقعی crss7777 و gektar در دست نیست.

خوشبختانه در هر دو مورد در مدتی کوتاه برخی شرکت‌های ضدویروس با بهره‌گیری از کلیدهای فاش شده اقدام به ساخت و انتشار ابزار رمزگشایی فایل‌های رمز شده توسط این دو نسخه نمودند.


شکل ۱۵: انتشار ابزارهای رمزگشایی بر اساس کلیدهای فاش شده

## نتیجه‌گیری

متأسفانه علیرغم عرضه برخی کلیدهای رمزگشایی این باج‌افزار، روند انتشار نسخه‌های جدید نه تنها متوقف نشده که با سرعت بیشتری در جریان است. آسان‌ترین و ارزان‌ترین راه در مقابله با این تهدیدات مخرب رعایت اقدامات پیشگیرانه زیر است.

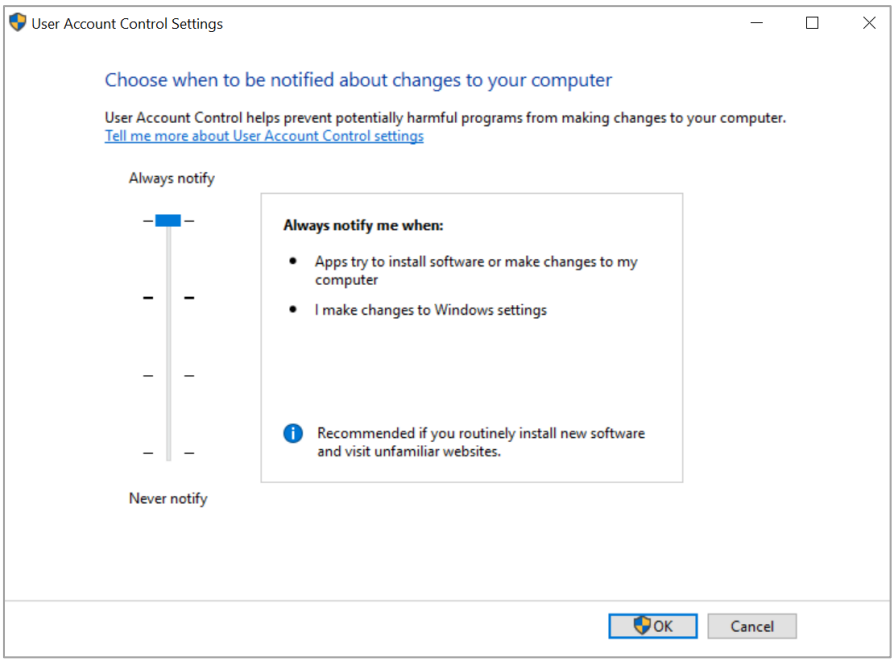
### ۱ تهیه نسخه پشتیبان

از اطلاعات سازمانی به‌صورت دوره‌ای نسخه پشتیبان تهیه شود. پیروی از قاعده ۳-۲-۱ برای داده‌های حیاتی توصیه می‌شود. بر طبق این قاعده، از هر فایل سه نسخه می‌بایست نگهداری شود (یکی اصلی و دو نسخه به‌عنوان پشتیبان). فایل‌ها باید بر روی دو رسانه ذخیره‌سازی مختلف نگهداری شوند. یک نسخه از فایل‌ها می‌بایست در یک موقعیت جغرافیایی متفاوت نگهداری شود. همچنین رمزگذاری فایل‌های پشتیبان برای حفاظت از آنها در برابر افراد غیرمجاز نیز توصیه می‌شود.

### ۲ محدود کردن سطح دسترسی

همه کاربران، حتی مدیر سیستم می‌بایست با حداقل سطح دسترسی مورد نیاز به هر سیستم وارد شوند. در صورت محدود بودن سطح دسترسی حتی در صورت اجرای فایل مخرب توسط کاربر، دستگاه به باج‌افزار آلوده نخواهد شد. همچنین برخی محصولات کنترل برنامه نظیر McAfee Application Control نیز می‌توانند به‌نحوی مؤثر از اجرا شدن فایل‌های غیرمجاز از جمله باج‌افزارها جلوگیری کنند.

همچنین توصیه می‌شود بخش User Account Control Settings در حالت Always notify me قرار داده شود.




شکل ۱۶: تنظیمات بخش User Account Control

برای اعمال این پیکربندی بر روی تمامی دستگاه‌های سازمان از طریق Group Policy می‌توان از این راهنما استفاده کرد.

## ۳ نصب اصلاحیه‌ها در اولین فرصت ممکن و استمرار در انجام آن

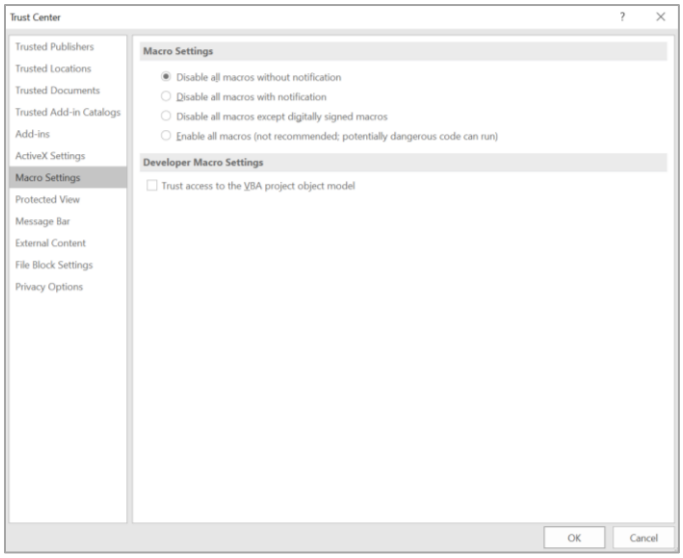
بسیاری از بهره‌جویی‌ها از طریق سوءاستفاده از ضعف‌های امنیتی نرم‌افزارهای پرکاربردی نظیر Adobe Flash، Office و مرورگرها صورت می‌پذیرد. هر چه زودتر اصلاحیه نصب شود آسیب کمتری متوجه سازمان می‌شود.

## ٤ استفاده از فناوری‌های حفاظتی پیشرفته

استفاده از ضدویروس قدرتمند و به‌روز جهت مقابله با باج‌افزارهای رمزگذار ضروری است. اما در کنار آن می‌بایست از راهکارهای نفوذیاب، ضدهرزنامه، کنترل‌کننده وب و دیواره آتش نیز استفاده کرد. همچنین برخی محصولات امنیتی نظیر McAfee و Bitdefender دارای راهکارهایی ویژه و خاص برای شناسایی و مقابله با باج‌افزارهای رمزگذار هستند.

## ۵ غیرفعال کردن بخش ماکرو

با توجه به انتشار بخش قابل توجهی از باج‌افزارها از جمله Sage از طریق فایل‌های نرم‌افزار Office حاوی ماکروی مخرب، غیرفعال کردن بخش ماکرو برای کاربرانی که به این قابلیت نیاز کاری ندارند با فعال کردن گزینه Disable all macros without notification توصیه می‌شود.




شکل ۱۷: تنظیمات امنیتی بخش ماکرو در نرم‌افزار Office

برای غیرفعال کردن این قابلیت، از طریق Group Policy، می‌توان از این راهنما و این راهنما استفاده کرد.

همچنین توصیه می‌شود ایمیل‌های دارای پیوست ماکرو در همان درگاه شبکه مسدود شوند. بدین منظور می‌توان از تجهیزات دیواره آتش مجهز به این قابلیت بهره گرفت.

## ٦ محدود کردن دسترسی از طریق پودمان RDP

مسدود نمودن دسترسی از طریق پودمان RDP بر روی آن دسته از دستگاه‌هایی که استفاده از آنها از طریق این پودمان ضرورتی ندارد توصیه می‌شود. همچنین توصیه می‌شود دسترسی به پوشه‌های اشتراکی و Clipboard از طریق این پودمان غیرفعال شود. برای این منظور می‌توان از این راهنما استفاده کرد. ضمن اینکه به تمامی کاربران، به خصوص به کاربران با حق دسترسی بالاتر می بایست گذرواژه‌ای پیچیده تخصیص داده شود. تغییر شماره درگاه پیش فرض RDP از دیگر نکاتی است که مدیران شبکه می‌بایست آن را مدنظر قرار دهند.

شایان ذکر است هر گونه تلاش برای اتصال به دستگاه از طریق RDP در سوابق با شناسه[۱۸] 1149 در بخش Event Viewer ضبط و نگهداری می‌شود.

## ۷ احتیاط در زمان باز کردن ایمیل‌ها

آموزش و راهنمایی کاربران سازمان به صرف‌نظر کردن از فایل‌های حتی کمی مشکوک و باز نکردن آنها می‌تواند نقشی مؤثر در پیشگیری از اجرا شدن پیوست‌های مخرب داشته باشد. برای این منظور می‌توانید از این داده‌نمایی‌ها استفاده کنید.

## ۸ به روز بودن در خصوص روش‌های جدید باج‌گیران

نویسندگان باج‌افزار دائماً در حال تغییر و تکامل روش‌های خود هستند. با مرور اخبار و حضور در دوره‌های آگاهی‌رسانی شرکت مهندسی شبکه گستر، از آخرین روش‌های مورد استفاده مهاجمان آگاه شده و سیاست‌ها پیشگرانه لازم را اعمال کنید.

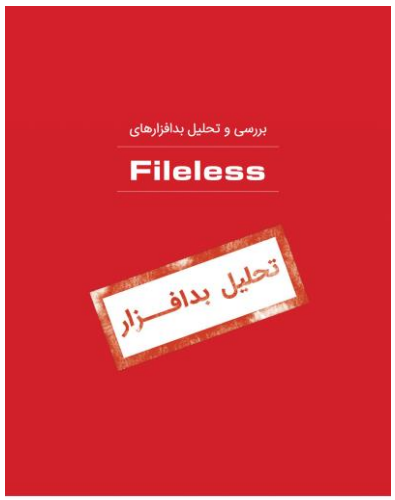
[۱۸] Event ID

## پیوست – نمونه‌های بررسی شده

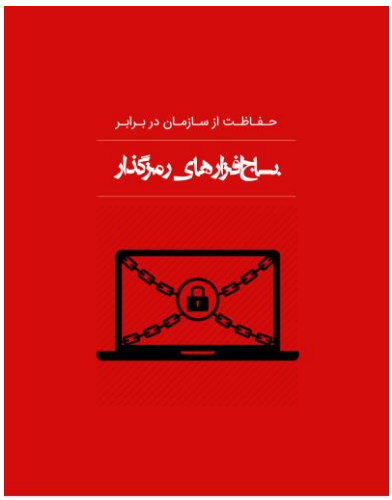
| درهم ساز MD5 | نام شناسایی | | |
|---|---|---|---|
| | McAfee | Bitdefender | ESET |
| c51b0e090ea08b0bbf5e504f74cd8409 | RDN/Ransom | Trojan.GenericKD.3457424 | Win32/Filecoder.Crysis.F |
| b5362a7afe85761a5b058bd2a2f0677a | Trojan-FJKH!B5362A7AFE85 | Trojan.GenericKD.3474055 | Win32/Filecoder.Crysis.E |
| b08a61e6a95438f384a5c45f6fdcca97 | RDN/Ransom | Trojan.GenericKD.3473684 | Win32/Filecoder.Crysis.F |
| db2a372dfcaa0dbba4aaff2eaeb5e516 | Generic.aih | Gen:Variant.Razy.91822 | Win32/Filecoder.Crysis.H |
| 677470da096fd251e423187285d36278 | Generic.agw | Trojan.Generic.17942761 | Win32/Filecoder.FS |
| 628296cb1c11b760bc420721c316a6a7 | Artemis!628296CB1C11 | Trojan.GenericKD.3516955 | Win32/Filecoder.Crysis.H |
| 60d54d3c75a9e6b84e7d625daa539a08 | Trojan-FJNQ!60D54D3C75A9 | Trojan.RanSerKD.3508506 | a variant of Win32/Kryptik.FGLW |
| b439be7f65128ac964564cfd2f123cb0 | GenericRXAO-OT!B439BE7F6512 | Trojan.GenericKD.3708467 | a variant of Win32/GenKryptik.KNR |
| b547e8a6510411aa4fb133fa577d3ce3 | Ransom-FBV!B547E8A65104 | Gen:Variant.Ransom.Crysis.6 | a variant of Win32/Filecoder.Crysis.L |

## منابع


- https://www.bleepingcomputer.com/news/security/number-of-rdp-brute-force-attacks-spreading-crysis-ransomware-doubles-in-6-months
- http://www.pandasecurity.com/mediacenter/malware/ransomware-crysis
- http://blogs.quickheal.com/troldesh-ransomware-brute-forcing-its-way-into-systems
- https://www.bleepingcomputer.com/forums/t/632389/dharma-ransomware-filenameemaildharmawalletzzzzz-support-topic/page-50
- http://www.trendmicro.co.uk/vinfo/uk/security/news/cybercrime-and-digital-threats/crysis-to-take-over-teslacrypt
- https://blog.avast.com/avast-releases-four-free-ransomware-decryptors
- https://www.bleepingcomputer.com/news/security/number-of-rdp-brute-force-attacks-spreading-crysis-ransomware-doubles-in-6-months
- http://newsroom.shabakeh.net/18046/eset-crysis-decryption-tool.html
- http://newsroom.shabakeh.net/18371/dharma-ransomware-decryptor-tool.html
- http://www.virusradar.com/en/Win32_Filecoder.Crysis.B/description
- http://www.welivesecurity.com/2016/11/24/new-decryption-tool-crysis-ransomware
- http://www.welivesecurity.com/2016/06/07/beyond-teslacrypt-crysis-family-lays-claim-parts-territory
- http://newsroom.shabakeh.net/18352/iranian-servers-are-targeted-by-ransomware.html
- https://www.certcc.ir
- http://blog.trendmicro.com/trendlabs-security-intelligence/crysis-targeting-businesses-in-australia-new-zealand-via-brute-forced-rdps
- http://blog.trendmicro.com/trendlabs-security-intelligence/brute-force-rdp-attacks-plant-crysis-ransomware






## شبکه گستر

شرکت مهندسی شبـکه گستر که در سال ۱۳۷۰ تأسیس گردیده، اولیـن شـرکت ایـرانـی است کـه در زمینه نرم‌افزارهای ضـدویـروس فعـالیت تخصصی و متمـرکـزی را آغـاز کـرد. در ابتـدا، همکـاری مشتـرکی بیـن شرکت مهندسی شبـکه گستـر و شرکت انگلیسی S & S International (تولیدکننده ضدویروس مشهور Toolkit) آغاز گردید. در مدت کوتاهی، با فعالیت شبکه گستر به‌عنوان نماینده رسمی و انحصاری S & S International در ایران، بـه تـدریج ضدویروس Dr Solomon's Toolkit به محبوب‌ترین ضدویروس در ایران تبدیل شد. پس از خرید شرکت S & S International توسط شرکت McAfee در سـال ۱۳۷۷، شرکت شبکه گستر نیز مانند دیگر نمـاینـدگان بیـن‌المللی فعـالیت خود را بر روی نرم‌افزارهای ضدویروس McAfee ادامه داد. در حال حاضر نیز شـرکت شبکه گستر به‌عنوان فروشنده مجاز ( Authorized Reseller) در منطقه خاورمیانه، به ارائه محصولات و خدمات درایران اقدام می نماید.

در سـال ۱۳۸۴ شـرکت مهندسی شبـکه گستر مـوفـق بـه کسب نـمـایـنـدگی رسمـی و انحصـاری شـرکت آلمانی Astaro، سـازنـده محصولات "مـدیریت یکپـارچـه تهـدیـدات" ( Unified Threat Management) گردید. به دنبال رشد چشمگیر و موفقیت جهانی محصولات امنیتی شرکت Astaro، در سال ۱۳۹۰ شرکت Sophos انگلیس، اقدام به خرید این شرکت آلمانی نمود. به دنبال این نقل و انتقال، شرکت مهندسی شبکه گستر به‌عنوان نماینده شرکت Sophos ادامه فعالیت داده و اکنون محصولات Astaro سابق را تحت نام جدید Sophos و دیگر محصولات امنیت شبکه این شرکت را در ایران عرضه می‌نماید.

از سال ۱۳۹۱ نیز، شرکت مهندسی شبکه گستر عرضه محصولات ضد ویروس Bitdefender را به‌عنوان نماینده و توزیع‌کننده (Distributor) رسمی در ایران، آغاز کرد. عرضه محصولات ضدویروس Bitdefender در کنار محصولات امنیتی McAfee، پاسخی به شرایط و نیازهای متفاوت کاربران و مدیران شبکه است. ضد ویروس چابک‌تر، مدیریت آسان‌تر و محصولی مقرون به صرفه‌تر، انتظاراتی بودند که برخی کاربران و مدیران شبکه‌های کوچک و متوسط داشتند و با عرضه محصولات ضدویروس Bitdefender، شبکه گستر به نیازهای این بخش از بازار پاسخ داد.

شرکت مهندسی شبکه گستر افتخار دارد که مجری برخی از بزرگترین و طولانی مدت‌ترین پروژه‌های طراحی، نصب، راه‌اندازی و پشتیبانی محصولات نرم‌افزاری ضدویروس و سخت‌افزاری فایروال در کشور بوده است.

این شرکت علاوه بر خدمات‌دهی به هزاران شرکت و سازمان که صدها هزار کاربر را در کشور شامل می‌شوند، دارای شبکه نمایندگی فروش و پشتیبانی در سراسر کشور نیز می‌باشد.

CSQ
ISO 9001:2008
Cert No 9150.C528

شبکه گستر

شرکت مهندسی شبکه گستر


تهران ۱۹۶۸۶، خیابان شهید دستگردی، شماره ۲۷۳

| | |
|---|---|
| تلفن / دورنگار | ۰۲۱-۴۲۰۵۲ |
| تارنمای شرکت | www.shabakeh.net |
| سامانه پشتیبانی | help.shabakeh.net |
| خدمات پس از فروش | my.shabakeh.net |
| مرکز آموزش | events.shabakeh.net |
| اتاق خبر | newsroom.shabakeh.net |