بـررسـی و تـحلیل بـدافـزار

# GAZER

شبکه گستر
امنیت شما | وظیفه ما

عنوان سند: بررسی و تحلیل بدافزار Gazer
شناسه سند: SPT-A-0142-00
تهیه‌کننده: گروه تحقیق و توسعه، شرکت مهندسی شبکه گستر
تاریخ ویرایش: ۲۵ شهریور ۱۳۹۶

```
TRUE            EQU     01H
FALSE           EQU     00H
BREAKINT        EQU     23H
GETVECTOR       EQU     35H
SETVECTOR       EQU     25H
DOS_FUNCTION    EQU     21H

BREAK           SEGMENT PUBLIC  'CODE'
BREAKFLAG       DB      0H
SAVEBRK         DD      0H
                ASSUME  CS:BREAK
                ASSUME  DS:NOTHING

                PUBLIC  CHECK_BREAK
CHECK_BREAK     PROC    FAR
                XOR     AX, AX
                MOV     AL, BREAKFLAG
                MOV     BREAKFLAG, FALSE
                RET
CHECK_BREAK     ENDP

                PUBLIC  INST_BRK_HANDLR
INST_BRK_HANDLR PROC    FAR
                PUSH    DS
                MOV     AL, BREAKINT
                MOV     AH, GETVECTOR
                INT     DOS_FUNCTION
                MOV     WORD PTR SAVEBRK
                MOV     WORD PTR SAVEBRK+2
                MOV     AL, BREAKINT
                MOV     AH, SETVECTOR
                MOV     DX, OFFSET
                MOV     BX, CS
                MOV     DS, BX
                INT     DOS_FUNCTION
                POP     DS
                RET
INST_BRK_HANDLR ENDP
REM_BRK_HANDLR  PROC    FAR
                PUSH    DS
                MOV     AL, BREAKINT
                MOV     AH, SETVECTOR
                MOV     DX, WORD PTR SAVEB
                MOV     BX, WORD PTR SAVEB
                MOV     DS, BX
                INT     DOS_FUNCTION
                POP     DS
                RET
REM_BRK_HANDLR  PROC    FAR
                PUSH    DS
                MOV     AL, BREAKINT
                MOV     AH, SETVECTOR
                MOV     DX, WORD PTR SAVEB
                MOV     BX, WORD PTR SAVEB
                MOV     DS, BX
                INT     DOS_FUNCTION
                POP     DS
                RET
REM_BRK_HANDLR  ENDP
BREAK           ENDS
                END
REM_BRK_HANDLR  PROC    FAR
                PUSH    DS
                MOV     AL, BREAKINT
                MOV     AH, SETVECTOR
                MOV     DX, WORD PTR SAVEB
                MOV     BX, WORD PTR SAVEB
                MOV     DS, BX
                INT     DOS_FUNCTION
                POP     DS
                RET
REM_BRK_HANDLR  ENDP
```

# فـهـرسـت مـطـالب

# مـعـرفـی

در شهریور ماه ۱۳۹۶، شرکت ESET از شناسایی یک حمله سایبری جاسوسی خبر داد که گردانندگان آن از سال ۲۰۱۶ میلادی کنسولگری‌ها، وزارتخانه‌ها و سفارتخانه‌ها را در کشورهای مختلف به ویژه کشورهای اروپای جنوب شرقی هدف قرار می‌داده‌اند.

در جریان این حملات، از یک بدافزار درب‌پشتی با نام Gazer برای جاسوسی از دولت‌ها و دیپلمات‌های آنها استفاده شده است.

به نظر می‌رسد این بدافزار توسط گروه Turla توسعه داده شده که در حملات پیشین ارتباط آن با سازمان‌های اطلاعاتی روسیه به اثبات رسیده بوده.

مهاجمان، Gazer – که به زبان C++ نوشته شده – را از طریق ایمیل‌های فیشینگ و سیستم‌های آسیب‌پذیر بر روی اهداف خود گسترش داده‌اند.

مکانیزم آلوده کردن سیستم‌ها در دو مرحله انجام می‌شود. در مرحله اول بدافزار، یک درب‌پشتی دیگر به نام Skipper را دریافت کرده و سپس کدهای آلوده Gazer را بر روی سیستم قربانی نصب می‌کند. گروه Trula در حملات گذشته نیز از درب‌پشتی Skipper استفاده کرده بوده.

در مرحله دوم نیز درب‌های پشتی Carbon و Kazuar بر روی سیستم قربانی نصب می‌شود.

نویسندگان Gazer برای مخفی ماندن و شناسایی نشدن توسط محصولات ضدبدافزار و دیواره آتش، از سایت‌های آسیب‌پذیر به عنوان پیشکار استفاده کرده‌اند. بر روی اکثر این سایت‌های تسّخیر شده سامانه مدیریت محتوای WordPress در حال اجرا بوده است.

Gazer از روش تزریق کد آلوده، برای کنترل سیستم قربانی ؤ پنهان ماندن طولانی مدت در زمان جمع‌آوری اطلاعات استفاده می‌کند.

همچنین می‌تواند دستورات دریافت شده توسط یک سیستم آلوده شده را به یک سیستم دیگر در همان شبکه ارسال کند.

تا کنون چهار گونه از Gazer شناسایی شده است. نسخه‌های قبلی Gazer با یک گواهی‌نامه معتبر صادر شده توسط شرکت Comodo برای شرکت Solid Loop Ltd امضاء شده بودند. Gazer در آخرین نسخه با یک گواهی‌نامه SSL برای شرکت Ultimate Computer Support Ltd امضاء شده است.

---

[۱] Backdoor
[۲] Vulnerable
[۳] Proxy
[۴] Code Injection

## ارتباط با گروه Trula

بدافزار Gazer از بسیاری جهات با سایر بدافزارهای گروه Trula شباهت دارد. در واقع بدافزارهای Gazer، Carbon و Kazuar می‌توانند فرامین رمزنگاری شده را از سرور فرماندهی دریافت کرده و بر رُوی سیستم آلوده یا سایر سیستم‌های داخل شبکه اجرا کنند. تمامی بدافزارهای یاد شده از ظرف رمزنگاری شده برای نگهداری اجزا و تنظیمات بدافزار استفاده می‌کنند. همچنین سوابق مربوط به فعالیت‌های خود را در یک فایل ذخیره می‌کنند.

فهرست سرورهای فرماندهی به صورت توکار و رمزنگاری شده در کد بدافزار Gazer درج شده‌اند. گروه Trula به صورت معمول از سایت‌های مجاز و معروف که به آنها نفوذ شده به عنوان اولین لایه Proxy و مخفی ماندن استفاده می‌کند.

در هر سه بدافزار فهرست مشابهی از پروسه‌ها وجود دارد که بدافزار آنها را جهت تزریق کد آلوده و برقراری ارتباط با سرور فرماندهی هدف قرار می‌دهد. طراحی این بدافزارها به گونه‌ای است که پروسه هدف بر اساس برنامه‌های نصب شده بر روی سیستم قربانی از فهرست پروسه‌ها انتخاب می‌شود.

## رمزنگاری اختصاصی

نویسندگان Gazer به صورت گسترده‌ای از رمزنگاری استفاده کرده‌اند. آنها بجای بکارگیری Windows Crypto API و کتابخانه‌های عمومی رمزنگاری، از کتابخانه‌های نوشته شده توسط خودشان برای عملیات رمزنگاری بهره گرفته‌اند.

کلیدهای RSA توکاری که در کد آنها وجود دارد شامل کلید عمومی و کلید خصوصی مهاجمان می‌شود. از کلید عمومی[۹] برای رمزنگاری اطلاعات ارسالی به سرور فرماندهی و از کلید خصوصی برای رمزگشایی اطلاعات دریافتی استفاده می‌شود. در نمونه‌های مختلف بدافزار، این کلیدها یکسان و مشابه نبوده‌اند. [۱]

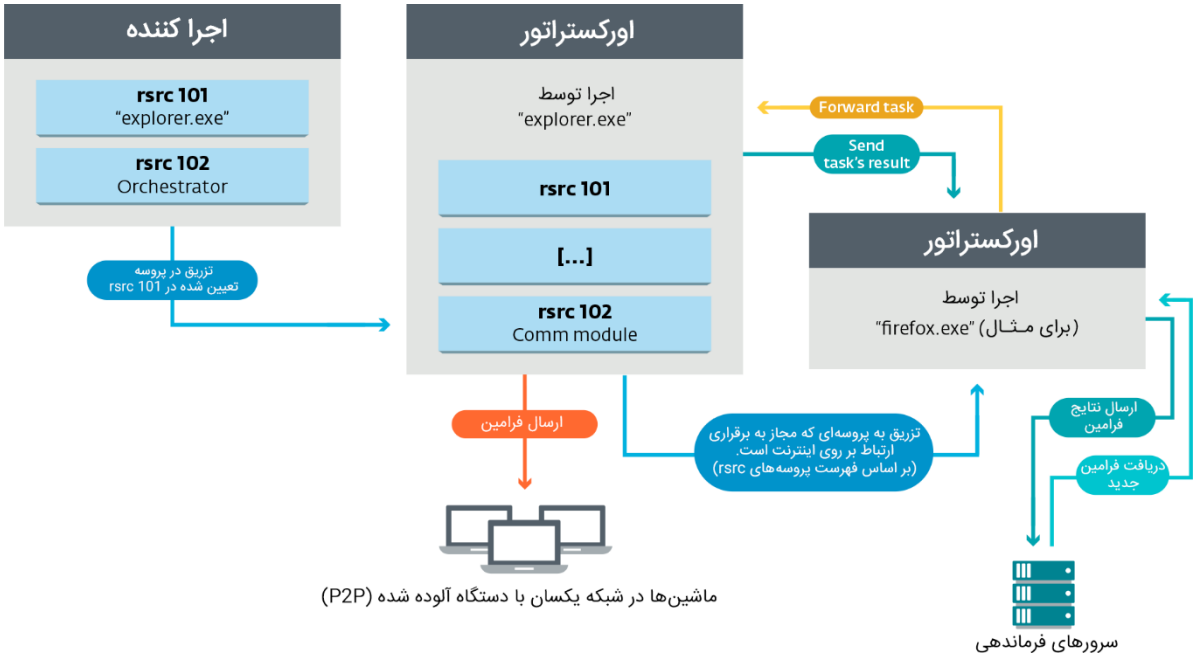
## اجـزاء

Gazer از اجزای زیر تشکیل شده است:

- اجـراکننده
- اورکستراتور

---

[۵] Encrypted Commands
[۶] Command and Control – C2
[۷] Container
[۸] Embedded
[۹] Public Key
[۱۰] Private Key




شکل ۱- اجزای Gazer

## اجرا کننده

اجرا کننده اولین جزئی از بدافزار است که بر روی سیستم اجرا می‌شود. کدهای زیر در یک فایل دودویی بدون رمزنگاری شدن ذخیره می‌شوند.

- 101: the process name to inject the orchestrator into
- 102: the orchestrator

## Named Pipe

جهت برقراری کانال ارتباطی میان اجزای Gazer، به یک Named Pipe نیاز است. Named Pipe از طریق رشته زیر ایجاد می‌شود:

- \\\\.\\pipe\\Winsock2\\CatalogChangeListener-FFFF-F

که در آن، عبارت FFFF-F با مقدار شناسه امنیتی کاربری که در حال استفاده از سیستم است، جایگزین می‌شود.

Loader
Binary
Security ID (SID)

## تزریق‌کننده

روش تزریق کد آلوده به پروسه، به صورت از راه دور چندان مرسوم نیست و بجای آن یک ریسه[1] از پروسه در حال اجرا، جهت اجرای اولیه ماژول ارتباطی، به صورت زیر، آلوده می‌شود:

- ماژول و ShellCode آلوده در پروسه کپی می‌شوند.
- از تابع ZwQuerySystemInformation جهت یافتن تعداد ریسه‌های در حال اجرای پروسه هدف قرار گرفته شده استفاده می‌شود.
- عملیات زیر بر روی هر ریسه انجام می‌شود:
  - ریسه توسط توابع OpenThread/SuspendThread متوقف می‌شود.
  - متن ریسه توسط GetThreadContext استخراج می‌شود.
  - اشاره‌گر دستورالعمل‌های متنی ذخیره شده و سپس اشاره‌گر از طریق SetThreadContext به ShellCode آلوده اشاره می‌کند.
  - ریسه مجدداً از طریق ResumeThread اجرا می‌شود.
- اگر هر یک از عملیات قبلی با موفقیت انجام نشود، ریسه مجدداً اجرا شده و اقدامات مشابه بر روی ریسه دیگر انجام می‌شود.

```
launcher:
   push rax
   sub rsp, 38h
   movabs rax, 5D20092              ; @ end of payload
   mov qword ptr ss:[rsp+28], rax   ; lpThreadId
   mov qword ptr ss:[rsp+20], 0     ; dwCreationFlags
   xor r9d, r9d                     ; lpParameter
   movabs r8, 5D20046               ; lpStartAddress => @payload
   xor edx, edx                     ; dwStackSize = 0
   xor ecx, ecx                     ; lpThreadAttributes = NULL
   call qword ptr ds:[CreateThread]
   movabs rax, 90A7FACE90A7FACE     ; replaced by the saved
                                    instruction pointer from
                                    thread context ;)
   add rsp, 38h
   xchg qword ptr ss:[rsp], rax
   ret

payload:
   sub rsp, 28
   movabs r8, 5D20096
   mov edx, 1
   movabs rcx, 4000000000000000
   call qword ptr ds: [DllEntryPoint]
   xor ecx, ecx
   call ExitThread
   int 3
   xxxx;  @DllEntryPoint
   xxxx ; @CreateThread
   xxxx; @ExitThread
   xxxx
   xxxx
   xxxx
   xxxx ; TID
```

شکل ۲ – ShellCode اجراکننده که ماژول آلوده را اجرا می‌کند

[1] Thread

Gazer از ۵ روش برای اجرای بدون وقفه بر روی سیستم‌ها استفاده می‌کند.

### ۱- راه‌اندازی خودکار از طریق پوسته [۱] [۵]

در این روش، بدافزار در محضرخانه و از مسیر زیر مقدار کلید Shell را به %malware_pathfile%, explorer. exe تغییر می دهد.

- HKCU\Software\Microsoft\Windows NT\CurrentVersion\Winlogon

### ۲- راه‌اندازی خودکار از طریق محافظ صفحه [۱] [۷]

در این روش، Gazer تنظیمات مرتبط با محافظ صفحه را در محضرخانه جهت اجرای فایل‌های خود تغییر می‌دهد.

متغیر و کلیدهای زیر در مسیر HKCU\Control Panel\Desktop در محضرخانه ایجاد می‌شوند:

- SCRNSAVE.exe با مسیر اجرایی بدافزار
- مقدار ScreenSaveActive را به یک تغییر می‌دهد. محافظ صفحه فعال می‌شود.
- مقدار ScreenSaverIsSecure را به صفر تغییر می‌دهد. مشخص می‌کند که محافظ صفحه دارای گذرواژه نباشد.
- مقدار ScreenSaveTimeout با توجه به مقدار تعریف شده در کد بدافزار تنظیم می‌شود. مشخص می‌کند که سیستم چه مدت قبل از اجرای محافظ صفحه (در این حالت: بدافزار) در حالت بلااستفاده باشد. [۸]

### ۳- فرمان زمانبندی راه‌اندازی خودکار [۱] [۹]

در این روش یک فرمان زمانبندی ایجاد می‌شود. این فرمان از طریق رابط‌های COM با نام‌هایی همچون ITaskService و ITaskSettings ایجاد و تنظیم می‌شود.

برخی از اطلاعات مانند نام فرمان و شرح آن توسط کد بدافزار تعیین می‌شود. به عنوان مثال در یکی از نمونه‌ها فرمان زیر بر روی سیستم تنظیم شده است:

- %APPDATA%\Adobe\adobeup.exe Adobe Acrobat Reader Updater. This task was generated by Adobe Systems, Inc to keep your Adobe Software up-to-data. \Adobe\AcrobatReader.Adobe

که جزییات آن بشرح زیر می‌باشد:

- نام فرمان: Adobe Acrobat Reader Updater
- بخش اجرایی: APPDATA%\Adobe\adobeup.exe%
- شرح فرمان: This task was generated by Adobe Systems, Inc to keep your Adobe Software up-to-data
- پوشه قرارگیری فرمان: Adobe\AcrobatReader.Adobe\

---

[۱] ShellAutorun
[۱] Windows Registry
[۱] ScreenSaverAutorun
[۱] Idle
[۱] TaskSchedulerAutorun

این فرمان علاوه بر اجرا در زمانبندی‌های مشخص شده، پس از ورود کاربر به سیستم نیز اجرا خواهد شد.

### ۴- فرمان مخفی راه‌اندازی خودکار[۲]

این روش بسیار شبیه روش شماره ۳ است با این تفاوت که فرمان زمانبندی با استفاده از پرچم TASK_FLAG_HIDDEN از دید کاربر مخفی شده است.

### ۵- راه‌اندازی خودکار به صورت پیوند

در این روش بدافزار فایل‌های LNK موجود را جهت اجرای بدافزار از طریق cmd.exe تغییر می‌دهد. برای هر فایل LNK که در کد مشخص شده، نشان و پارامترهای آنها حذف و مسیر اجرا به مسیر زیر تغییر می‌کند:

- cmd.exe /q /c start %s && start %s

در بیشتر نمونه‌هایی که مورد تجزیه و تحلیل قرار گرفته، بدافزار برای اجرای بدون وقفه بر روی سیستم‌ها از روش ۳ استفاده کرده است.

### سوابق

سوابق اجزای اشاره شده در فایل‌های مجزایی به صورت رمزنگاری شده با الگوریتم 3DES، ذخیره می‌شوند.

در برخی از نسخه‌های Gazer، دستیابی به سوابق به راحتی امکان‌پذیر است زیرا مسیر ذخیره شدن سوابق در فایل دودویی آنها مشخص شده است.

برخی نمونه از این فایل‌ها عبارتند از:

- %TEMP%\CVRG72B5.tmp.cvr: سوابق مربوط به اجرا کننده
- %TEMP%\CVRG1A6B.tmp.cvr: سوابق مربوط به Orchestrator
- %TEMP%\CVRG38D9.tmp.cvr: سوابق مربوط به ماژول ارتباطی[۴]

هر کدام از فایل‌های سوابق ساختاری شبیه قالب زیر دارند:

[LOGSIZE][DECRYPTION_KEY][ENCRYPTED_LOG]

که در آن:

- Logsize مقدار ۲ بایتی بوده و اندازه سوابق رمزنگاری شده را مشخص می‌کند.
- Decryption_key مقداری ۱۲ بایتی بوده و با مکانیزم خاصی جهت رمزگشایی فایل لاگ را ایجاد می‌کند.
- Encrypted_log توضیحات سابقه که با استفاده از الگوریتم 3DES رمزگذاری شده است.

---

[۲] HiddenTaskAutorun
[۲] Flag
[۲] LinkAutorun
[۲] Log
[۲] Communication Module

```
|10:29:56:197|   [1556]
|10:29:56:197|   [1557]    *****************[...]***************
|10:29:56:197|   [1558]    DATE: 25.05.2017
|10:29:56:197|   [1559]    PID=900 TID=2324    Heaps=32
C:\Windows\Explorer.EXE
|10:29:56:197|   [1565]    DLL_PROCESS_ATTACH
|10:29:56:197|   [1574]    4164
|10:29:58:197|   [0137]    =================[...]===============
|10:29:58:197|   [0138]    Current thread = 2080
|10:29:58:197|   [0183]    Heap aff0000 [34]
|10:29:58:197|   [0189]    ### PE STORAGE ###
|10:29:58:197|   [0215]    ### PE CRYPTO ###
|10:29:58:197|   [0246]    ### EXTERNAL STORAGE ###
|10:29:58:197|   [1688]    Ok
|10:29:58:197|   [0279]    Path = \HKCU\Software\Microsoft\
Windows\CurrentVersion\Explorer\ScreenSaver
|10:29:58:197|   [0190]    \HKCU\Software\Microsoft\Windows\
CurrentVersion\Explorer\ScreenSaver
|10:29:58:197|   [0338]    ---FAILED
|10:29:58:197|   [0346]    Initializing standart reg storage...
|10:29:58:197|   [0190]    Software\Microsoft\Windows\
CurrentVersion\Explorer\ScreenSaver
|10:29:58:197|   [2605]    Storage is empty!
|10:29:58:197|   [0392]    ### EXTERNAL CRYPTO ###
|10:29:59:666|   [1688]    Ok
|10:29:59:713|   [1473]    Ok
|10:29:59:760|   [1688]    Ok
|10:29:59:775|   [1473]    Ok
|10:29:59:775|   [1688]    Ok
|10:29:59:775|   [1473]    Ok
|10:29:59:791|   [1688]    Ok
|10:29:59:791|   [1473]    Ok
|10:29:59:806|   [1688]    Ok
|10:29:59:806|   [1473]    Ok
|10:29:59:806|   [0270]    08-00-27-90-05-2A
|10:29:59:806|   [0286]    _GETSID_METHOD_1_
|10:29:59:806|   [0425]    28 7 8 122
|10:29:59:806|   [0463]    S-1-5-21-84813077-3085987743-
2510664113-1000
|10:29:59:806|   [0471]
|10:29:59:806|   [0787]    Ok
|10:29:59:806|   [1473]    Ok
|10:29:59:822|   [0514]    ### QUEUES ###
|10:29:59:822|   [0370]    T Empty
|10:29:59:822|   [0482]    R Empty
|10:29:59:822|   [1754]    Ok
|10:29:59:822|   [1688]    Ok
|10:29:59:822|   [1473]    Ok
|10:29:59:838|   [0505]    R #4294967295 PR_100 TR_00000000
SZ_172 SC_0(50)  --+-       EX_0
|10:29:59:838|   [0625]    ### TRANSPORT ###
|10:29:59:838|   [0286]    _GETSID_METHOD_1_
|10:29:59:838|   [0425]    28 7 25 122
|10:29:59:838|   [0463]    S-1-5-21-84813077-3085987743-
2510664113-1000
|10:29:59:838|   [0471]
|10:29:59:838|   [0165]    \\.\pipe\Winsock2\
CatalogChangeListener-2313-4
|10:29:59:838|   [0131]    PipeName = \\.\pipe\Winsock2\
CatalogChangeListener-2313-4
|10:29:59:838|   [0041]    true
[...]
```

شکل ۳ – نمونه‌ای از سابقه رمزگشایی شده

## اورکستراتور

فایل‌های مورد نیاز Gazer به عنوان منابع Orchestrator ذخیره می‌شوند.

به صورت کلی ۱۱ منبع وجود دارد که ساختار زیر در آنها رعایت شده است:

[DATATYPE][SIZE][DATA][PADDING]

که در آن:

- DATATYPE: یک dword است که نوع داده‌های زیر را در منبع مشخص می‌کند:

- 0x0: داده خام
- 0xFFFFFFFF: تهی
- 0x4: تعریف نشده
- 0x1030001: آرایه‌ای از رشته‌ها
- 0x1: دودویی

- SIZE: اندازه داده‌ها (بدون Padding)

## منابع

همچنین فهرست منابع آن نیز بشرح زیر است:

- 101: کلید خصوصی. از این کلید برای رمزگشایی سایر منابع استفاده می‌شود.
- 102: کلید عمومی
- 103: تهی
- 104: تعریف نشده
- 105: اطلاعات پایدار را ذخیره می‌کند.
- 106: فهرستی از پروسه‌هایی که برای تزریق کد ماژول ارتباطی استفاده می‌شوند.
- 107: DLL ارتباط با سرور فرماندهی
- 108: فهرست سرور فرماندهی
- 109: مسیرهای مورد استفاده Gazer
- 110: فهرست افزونه‌ها
- 111: اطلاعات ارتباطات داخلی

تمامی منابع بالا بجز موارد 101 و 102 از طریق BZip فشرده شده و با الگوریتم 3DES رمزنگاری شده‌اند.

## فرامین اجرایی

فرامین اجرایی که می‌تواند از سرور فرماندهی دریافت شوند، عبارتند از:

- بارگذاری فایل
- دریافت فایل
- به‌روزرسانی تنظیمات
- اجرای دستورات

نتیجه فرامین در یک صف ذخیره شده و جهت ارسال به سرور فرماندهی در اختیار ماژول ارتباطی قرار می‌گیرد. ماژول ارتباطی نیز بمحض دسترسی به اینترنت با سرور فرماندهی ارتباط برقرار می‌کند.

### ماژول ارتباطی

ماژول ارتباطی جهت دریافت فرامین از سرور فرماندهی و انتقال آنها به Orchestrator استفاده می‌شود. کتابخانه‌های این بخش از بدافزار به پروسه‌هایی تزریق می‌شوند که توانایی برقراری ارتباط با اینترنت را دارند.

اگر Proxy در شبکه وجود داشته باشد، این ماژول اطلاعات آن را بازیابی کرده و بدین ترتیب با استفاده از آن می‌تواند در خواست‌های HTTP خود را ارسال کند. ماژول ارتباطی برای بازیابی اطلاعات Proxy از دو روش استفاده می‌کند.

در روش اول از اطلاعات درج شده در مسیر زیر در محضرخانه استفاده می‌شود:

- HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings

در روش دوم در صورتی که ماژول نتواند اطلاعات Proxy را از طریق روش اول بازیابی کند، تابع InternetQueryOption را با پرچم INTERNET_OPTION_PROXY فراخوانی می‌کند.

بدافزار قبل از اینکه با سرور فرماندهی ارتباط برقرار کند، اتصال اینترنت را از طریق دسترسی به سایت‌های زیر مورد بررسی قرار می‌دهد:

- update.microsoft.com
- microsoft.com
- windowsupdate.microsoft.com
- yahoo.com
- google.com

بدافزار Gazer با استفاده از روش HTTP GET دستورات را از سرور فرماندهی دریافت کرده و نتیجه اجرای فرامین را با روش HTTP POST برای سرور ارسال می‌کند.

```
xxx.php?album=2ildzq&key=hdr2a&partners=d2lic33f&session=nurvxd2x0z8bztz&video
=sg508tujm&photo=4d4idgkxxx.php?photo=he29zms5fc&user=hvbc2a&author=xvfj5r0q
9c&client=7mvvc&partners=t4mgmuy&adm=lo3r6v4xxx.php?member=ectwzo820&contact
=2qwi15&album=f1qzoxuef4&session=x0z8bztz8hrs65f&id=t3x0ftu9xxx.php?partners
=ha9hz9sn12&hash=5740kptk3acmu&album=uef4nm5d&session=dpeb67ip65f&member=arj6
x3ljjxxx.php?video=nfqsz570&client=28c7lu2&partners=818eguh70&contact=ibj3xch
&content=1udm9t799ixr&session=5fjjt61qred9uo
```

شکل ۴ – نمونه‌ای از درخواست HTTP درب‌پشتی Gazer

## نسـخ

در حال حاضر چهار گونه از این بدافزار شناسایی شده است.

در اولین نسخه نام واقعی توابع در فایل‌های سوابق ثبت و برای تزریق کد آلوده از دو روش استفاده شده است.

در نسخه دوم، بجای نام توابع، شناسه آنها در سوابق ثبت شده و فقط از یک روش برای تزریق کد آلوده استفاده گردیده است. همچنین عبارت NO OLD METHODS در کدهای این نسخه به چشم می‌خورد.

برخی نمونه‌های نسخه اولیه Gazer با یک گواهی‌نامه معتبر صادر شده توسط Comodo – برای شرکت Solid Loop Ltd – امضاء شده بودند. به نظر می‌رسد تاریخ تدوین گواهی‌نامه سال ۲۰۰۲ باشد اما احتمالاً به علت صدور آن در سال ۲۰۱۵، یک گواهی‌نامه جعلی است.

بدافزار Gazer در آخرین نسخه با گواهی‌نامه متعلق به شرکت Ultimate Computer Support Ltd امضاء شده است.

## نشانه‌های آلودگی

### فایل‌ها

- %TEMP%\KB943729.log
- %TEMP%\CVRG72B5.tmp.cvr
- %TEMP%\CVRG1A6B.tmp.cvr
- %TEMP%\CVRG38D9.tmp.cvr
- %TEMP%\~DF1E06.tmp
- %HOMEPATH%\ntuser.dat.LOG3
- %HOMEPATH%\AppData\Local\Adobe\AdobeUpdater.exe

### کلیدهای محضرخانه

- HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ScreenSaver
- HKCU\Software\Microsoft\Windows NT\CurrentVersion\Explorer\ScreenSaver

### نشانی‌های سرور فرماندهی

- daybreakhealthcare.co.uk/wp-includes/themees.php
- simplecreative.design/wp-content/plugins/calculated-fields-form/single.php
- 169.255.137.203/rss_0.php
- outletpiumini.springwaterfeatures.com/wp-includes/pomo/settings.php
- zerogov.com/wp-content/plugins.deactivate/paypal-donations/src/PaypalDonations/SimpleSubsribe.php
- ales.ball-mill.es/ckfinder/core/connector/php/php4/CommandHandler/CommandHandler.php
- dyskurs.com.ua/wp-admin/includes/map-menu.php
- warrixmalaysia.com.my/wp-content/plugins/jetpack/modules/contact-form/grunion-table-form.php
- 217.171.86.137/config.php

- 217.171.86.137/rss_0.php
- shinestars-lifestyle.com/old_shinstar/includes/old/front_footer.old.php
- www.aviasiya.com/murad.by/life/wp-content/plugins/wp-accounting/inc/pages/page-search.php
- baby.greenweb.co.il/wp-content/themes/san-kloud/admin.php
- soligro.com/wp-includes/pomo/db.php
- giadinhvabe.net/wp-content/themes/viettemp/out/css/class.php
- tekfordummies.com/wp-content/plugins/social-auto-poster/includes/libraries/delicious/Delicious.php
- kennynguyen.esy.es/wp-content/plugins/wp-statistics/vendor/maxmind-db/reader/tests/MaxMind/Db/test/Reader/BuildTest.php
- sonneteck.com/wp-content/plugins/yith-woocommerce-wishlist/plugin-fw/licence/templates/panel/activation/activation.php
- chagiocaxuanson.esy.es/wp-content/plugins/nextgen-gallery/products/photocrati_nextgen/modules/ngglegacy/admin/templates/manage_gallery/gallery_preview_page_field.old.php
- hotnews.16mb.com/wp-content/themes/twentysixteen/template-parts/content-header.php
- zszinhyosz.pe.hu/wp-content/themes/twentyfourteen/page-templates/full-hight.php
- weandcats.com/wp-content/plugins/broken-link-checker/modules/checkers/http-module.php

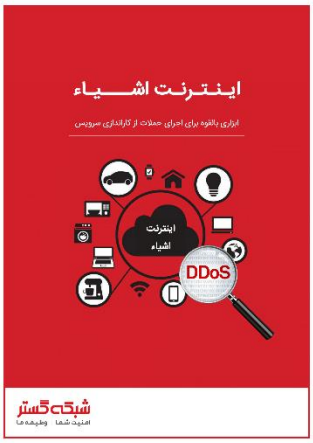
**درهم‌ساز**

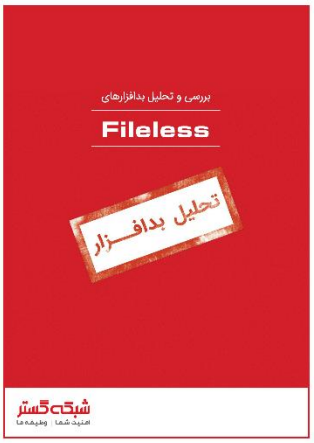
- 27fa78de705ebaa4b11c4b5fe7277f91906b3f92
- 35f205367e2e5f8a121925bbae6ff07626b526a7
- b151cd7c4f9e53a8dcbdeb7ce61ccdd146eb68ab
- e40bb5beec5678537e8fe537f872b2ad6b77e08a
- 267f144d771b4e2832798485108decd505cb824a
- 52f6d09cccdbc38d66c184521e7ccf6b28c4b4d9
- 22542a3245d52b7bcdb3eaef5b8b2693f451f497
- e05ab6978c17724b7c874f44f8a6cbfb1c56418d
- 6dec3438d212b67356200bbac5ec7fa41c716d86
- c3e6511377dfe85a34e19b33575870dda8884c3c
- 9ff4f59ca26388c37d0b1f0e0b22322d926e294a
- bae3ae65c32838fb52a0f5ad2cde8659d2bff9f3
- 8184ad9d6bbd03e99a397f8e925fa66cfbe5cf1b
- 7ced96b08d7593e28fee616eccbc6338896517cf
- 63c534630c2ce0070ad203f9704f1526e83ae586
- 11b35320fb1cf21d2e57770d8d8b237eb4330e
- e8a2bad87027f2bf3ecae477f805de13fccc0181
- a5eec8c6aadf784994bf68d9d937bb7af3684d5c
- 4b6ef62d5d59f2fe7f245dd3042dc7b83e3cc923

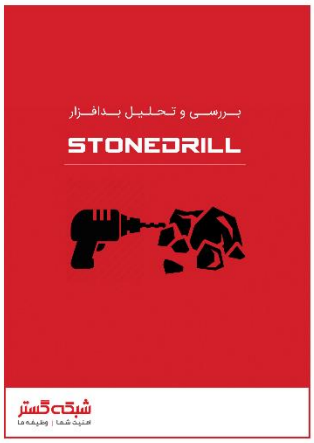
# منابع

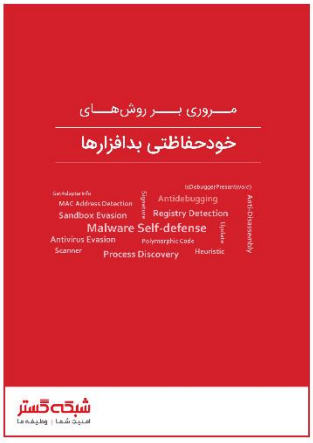

- https://www.welivesecurity.com/wp-content/uploads/2017/08/eset-gazer.pdf
- http://securityaffairs.co/wordpress/62518/apt/gazer-backdoor-apt-turla.html
- https://www.welivesecurity.com/2017/08/30/eset-research-cyberespionage-gazer
- http://thehackernews.com/2017/08/gazer-backdoor-malware.html

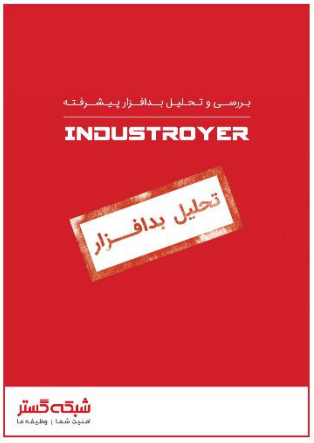

## در اتاق خبر شبکه گستر بخوانید...

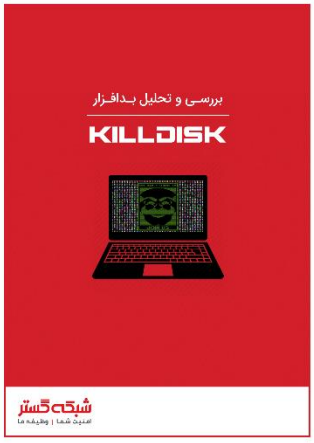


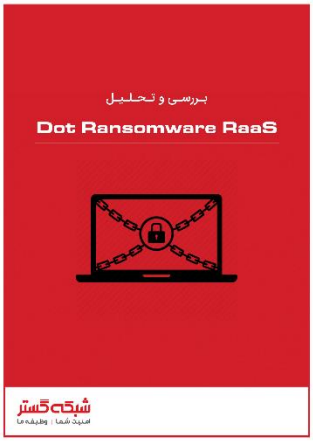



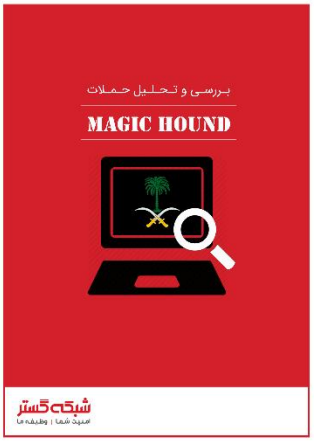



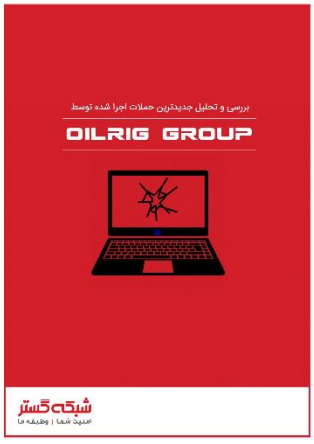



## شبکه گستر

شرکت مهندسی شبکه گستر در سال ۱۳۷۰ تأسیس گردید و اولین شرکت ایرانی است که در زمینه نرم‌افزارهای ضدویروس فعالیت تخصصی و متمرکزی را آغاز کرده است. در ابتدا، همکاری مشترکی بین شرکت مهندسی شبکه گستر و شرکت انگلیسی S & S International (تولیدکننده ضدویروس مشهور Toolkit) آغاز گردید. در مدت کوتاهی، با فعالیت شبکه گستر به عنوان نماینده رسمی و انحصاری S & S International در ایران، به تدریج ضدویروس Dr Solomon's Toolkit به محبوب‌ترین ضدویروس در ایران تبدیل شد.

پس از خرید شرکت S & S International توسط شرکت McAfee در سال ۱۳۷۷، شرکت شبکه گستر نیز مانند دیگر نمایندگان بین‌المللی فعالیت خود را بر روی نرم‌افزارهای ضدویروس McAfee ادامه داد. اکنون نیز شبکه گستر به عنوان فروشنده مجاز (Authorized Reseller) در منطقه خاورمیانه، به ارائه محصولات و خدمات در ایران اقدام می‌نماید.

در سال ۱۳۸۴ شرکت مهندسی شبکه گستر موفق به کسب نمایندگی رسمی شرکت آلمانی Astaro، سازنده محصولات مدیریت یکپارچه تهدیدات (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 با همکاری با شرکت Sophos، فعالیت خود را در این زمینه ادامه داده و اکنون محصولات Astaro سابق را تحت نام Sophos در ایران عرضه می‌نماید.

از سال ۱۳۹۱ شرکت مهندسی شبکه گستر عرضه محصولات ضدویروس Bitdefender را به عنوان 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 بوده است. ضد ویروس چابک‌تر، مدیریت آسان‌تر و محصولی مقرون به صرفه‌تر، انتظارات برخی از کاربران و مدیران شبکه بود که 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 پروژه‌های نصب و راه‌اندازی و طولانی مدت‌ترین قراردادهای نگهداری و پشتیبانی محصولات امنیت شبکه 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.

ISO 9001:2008
Cert No 9150.C528

اتـــاق خـبـــر

**newsroom**.shabakeh.net

مـرکـز آمـــوزش

**events**.shabakeh.net

خدمات پس از فروش

**my**.shabakeh.net

خدمات پشتیبانی فنی

**help**.shabakeh.net


شبکه گستر

شرکت مهندسی شبکه گستر

تهران خیابان شهید دستگردی (ظفر) شماره ۲۷۳

تلفن / دورنگار ۴۲۰۵۲ - ۰۲۱

info@shabakeh.net www.shabakeh.net