حفاظت از سازمان در برابر تهدیدات مبتنی بر

Remote Desktop Protocol

شبکه گستر

امنیت شما | وظیفه ما

مقدمه

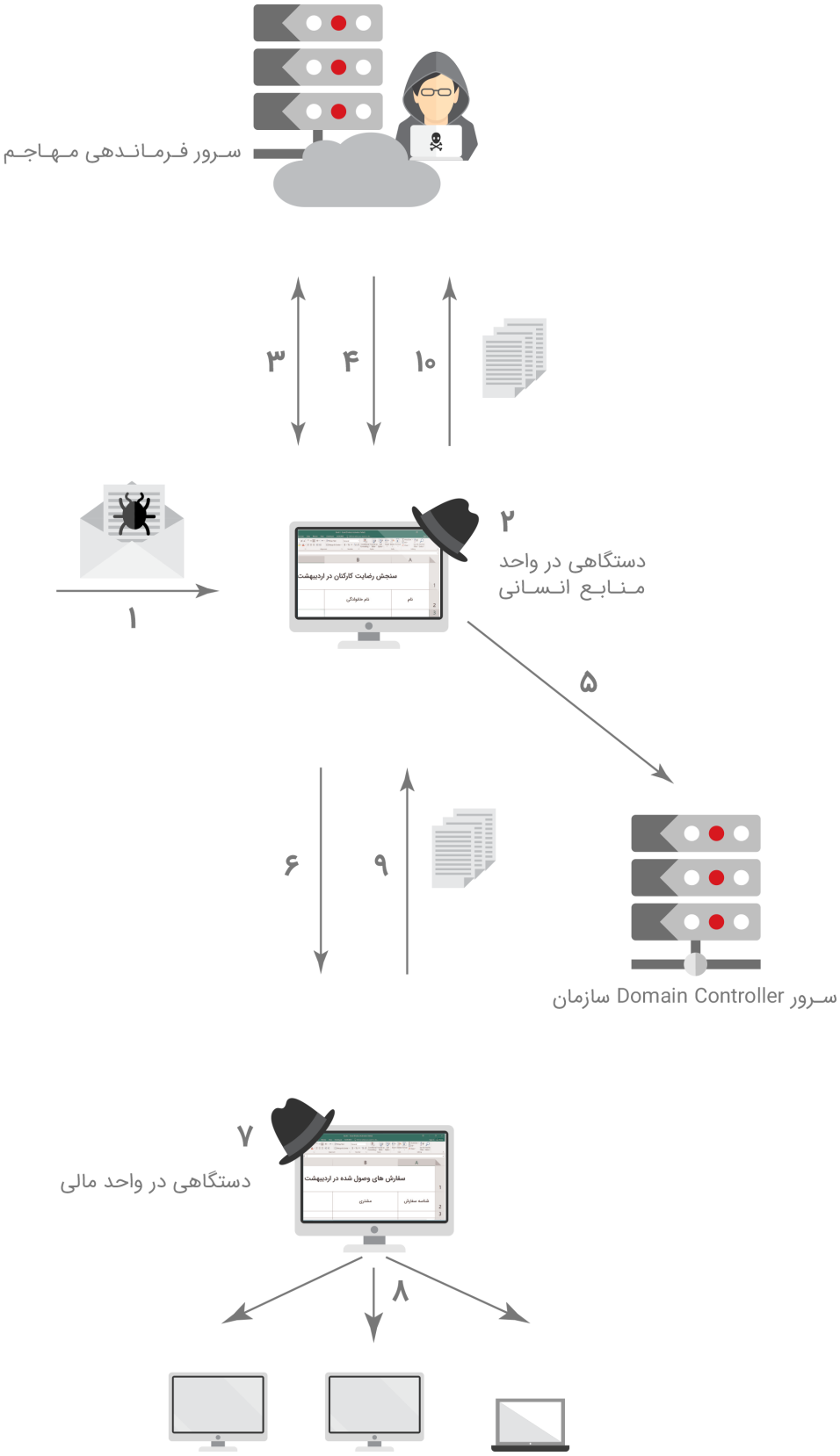
Remote Desktop Protocol – به اختصار RDP – از پودمان‌های پراستفاده در سیستم عامل Windows است. علاوه بر مدیران و راهبران شبکه که این پودمان را برای اتصال به سرورها و ایستگاه‌های کاری سازمان به کار می‌گیرند، در بسیاری از سازمان‌های کوچک و متوسط نیز از RDP برای برقرار نمودن ارتباط از راه دور پیمانکاران حوزه فناوری اطلاعات، به سرورهایی همچون حقوق و دستمزد، اتوماسیون اداری و غیره نیز استفاده می‌شود.

در سال‌های اخیر، مهاجمان برای انجام فعالیت‌های مخربی همچون انتشار انواع بدافزارها از جمله باج‌افزارها به‌طور گسترده‌ای از پودمان RDP بهره گرفته‌اند. به‌نحوی طی یک سال گذشته مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه‌ای کشور (ماهر) در چندین نوبت نسبت به سوءاستفاده مهاجمان از پودمان RDP برای آلوده‌سازی دستگاه‌ها به باج‌افزار هشدار داده است. این مرکز میانگین خسارت ناشی از هریک از این حملات را – بدون احتساب مبالغ احتمالی باج پرداخت شده توسط بعضی از قربانیان –، حدود نهصد میلیون ریال اعلام کرده است.

برای درک بهتر اینکه مهاجمان چگونه از قابلیت پودمان RDP بهره می‌گیرند، به مثال زیر و شکل ۱ توجه شود:

۱. یکی از کارکنان واحد منابع انسانی در دام یک ایمیل فریبنده افتاده و بدافزاری از نوع درب‌پشتی[۱] بر روی دستگاه سازمانی او نصب می‌شود.
۲. درب‌پشتی برای دستیابی به اطلاعات اصالت‌سنجی[۲] کاربرانی که به دستگاه قربانی دسترسی داشته‌اند و اطلاعات آنها در حافظه دستگاه ذخیره شده، ابزار Mimikatz را به اجرا در می‌آورد.
۳. درب‌پشتی یک تونل ارتباطی را با سرور فرماندهی[۳] مهاجم برقرار می‌کند.
٤. مهاجم از طریق تونل ایجاد شده و پودمان RDP و همچنین رمزعبوری که در مرحله دوم بدست آورده به دستگاه کارمند واحد منابع انسانی وارد می‌شود.
۵. مهاجم به‌منظور دستیابی به اطلاعات مالی از دستورات شمارشی[٤] Active Directory برای شناسایی دستگاه‌های واحد مالی عضو دامنه[۵] استفاده می‌کند.
٦. مهاجم از طریق پودمان RDP و با استفاده از اطلاعات اصالت‌سنجی کارمند واحد منابع انسانی که در مرحله دوم بدست آورده به یکی از دستگاه‌های شناسایی شده جدید متصل می‌شود.
۷. مشابه مرحله دوم، مهاجم با استفاده از Mimikatz اطلاعات اصالت‌سنجی ذخیره شده در حافظه دستگاه واحد مالی را استخراج می‌کند. به‌عنوان نمونه اطلاعات می‌تواند متعلق به کارمند واحد مالی یا مدیر سیستمی باشد که اخیراً برای رفع عیب دستگاه به آن وارد شده است.
۸. اکنون مهاجم از طریق پودمان RDP و با استفاده از حساب کاربری مدیر سیستم، کارمند واحد مالی و یا کارمند واحد منابع انسانی به دستگاه‌های دیگر داخل سازمان وارد می‌شود.
۹. مهاجم پس از شناسایی و جمع‌آوری اطلاعات باارزش، آنها را به‌طور موقت بر روی دستگاه کارمند واحد منابع انسانی که مبداء اتصالات RDP در شبکه سازمان هدف قرار گرفته شده است ذخیره می‌کند.
۱۰. در ادامه، مهاجم از طریق قابلیت Copy/Paste فعال شده در پودمان RDP اقدام به انتقال اطلاعات و فایل‌های ذخیره شده بر روی دستگاه واحد منابع انسانی به سیستم خود می‌کند.

۱ Backdoor
۲ Credential
۳ Command and Control - C2
٤ Enumeration Commands
۵ Domain



شکل ۱- نمونه‌ای از نفوذ از سرقت اطلاعات از طریق پودمان RDP

سند مرجع ارتباطات از راه دور

تهیه سند مرجع[1] ارتباطات RDP شبکه بهترین روشی است که می‌توان برای شناسایی این‌گونه فعالیت‌های مخرب به کار گرفت. برای انجام این امر، در ابتدا سازمان باید رفتار معمول واحدهای مختلف را شناسایی نموده و در ادامه شروع به پیکربندی چگونگی تشخیص الگوهای پیش‌بینی نشده کند. در زیر به برخی از سوالاتی که می‌تواند بر اساس مثال بالا به تعیین روش‌های تشخیص عملی کمک کند، اشاره شده است:

۱. آیا معمولا کارکنان واحد منابع انسانی و/یا مالی از پودمان RDP استفاده می‌کنند؟
۲. آیا کاربری از واحد منابع انسانی از طریق پودمان RDP به دستگاهی در واحد مالی متصل می‌شود؟
۳. آیا کاربری از واحد منابع انسانی یا مالی می‌تواند برای دسترسی به چندین دستگاه از پودمان RDP استفاده کند؟
٤. آیا از دستگاه‌های موجود در واحدهای مالی یا منابع انسانی می‌توان به عنوان دستگاه مبدا در پودمان RDP استفاده کرد؟
٥. آیا کاربران با سطح دسترسی بالا نظیر Administrator می‌توانند از طریق پودمان RDP و دستگاهی خارج از شبکه سازمان به دستگاه‌های داخل شبکه سازمان دسترسی داشته باشند؟
٦. آیا دستگاه‌هایی در خارج از شبکه سازمان می‌توانند با استفاده از پودمان RDP به سرورهای مهم و حیاتی داخل سازمان دسترسی از راه دور داشته باشند؟
۷. آیا کاربری از واحد منابع انسانی می‌تواند از طریق پودمان RDP به سرورهای مهم و حساس سازمان دسترسی داشته باشد؟
۸. آیا امکان آن وجود دارد که یک کاربر از چندین مبدا، آغازکننده ارتباطات مربوط به پودمان RDP باشد؟

توسعه یک فرآیند سفارشی شده جهت تعیین شاخص عملکرد حساب‌های کاربری و دستگاه‌های مبدا و مقصدی که می‌توانند از پودمان RDP در بستر سازمان استفاده کنند وقت‌گیر و زمان‌بر است. عادی‌سازی و بررسی این اطلاعات به کارکنان قدرت دید عمیق‌تر در زمینه شناسایی و توانایی بررسی سریع‌تر رفتارهای غیرمعمول کاربران در مواقع اضطراری را می‌دهد.

جستجو در سوابق ارتباطات RDP

در هنگام استفاده از پودمان RDP رویدادهایی در بخش Event Viewer سیستم عامل هر دو دستگاه مبدا و مقصد ایجاد می‌شود که در ادامه به آنها پرداخته شده است.

- رویدادهای با شناسه EID 21 و EID 25 موسوم به Remote Desktop Services Availability در بخش TerminalServices-LocalSessionManager که معمولا در مسیر زیر ذخیره می‌شوند:

%systemroot%\Windows\System32\winevt\Logs\Microsoft-TerminalServices-LocalSessionmanager%3Operational.evtx

- رویدادهای با شناسه EID 4624 موسوم به An account was successfully logged on از جنس Type 10 که معمولا در مسیر زیر ذخیره می‌شوند:

%systemroot%\Windows\System32\winevt\Logs\Security.evtx

هنگامی که کاربر محلی یا از راه دور به سیستم وارد می‌شود مطابق شکل ۲ رویدادی با شناسه EID 21 در دستگاه مقصد ثبت می‌شود.

[1] Baseline

ID:	21
Source:	Microsoft-Windows-TerminalServices-LocalSessionManager
Message:	Remote Desktop Services: Session logon succeeded: User: %1 Session ID: %2 Source Network Address: %3

شکل ۲ - نمونه‌ای از ساختار رویداد ثبت شده EID 21

اگر دستگاه مبدا مجددا از طریق پودمان RDP به دستگاه مقصد متصل شود ولی کاربر دستگاه مبدا از دستگاه مقصد خارج نشده و ارتباط RDP قبلی را به درستی پایان نداده باشد، در دستگاه مقصد رویدادی با شناسه EID 25 ایجاد می‌شود. به‌عنوان نمونه کاربر بجای خارج شدن از دستگاه از طریق منوی Start – که سبب ایجاد رویداد EID 23 می‌شود –، فقط پنجره RDP را ببندد.

ID:	25
Source:	Microsoft-Windows-TerminalServices-LocalSessionManager
Message:	Remote Desktop Services: Session reconnection succeeded: User: %1 Session ID: %2 Source Network Address: %3

شکل ۳ - نمونه‌ای از ساختار رویداد ثبت شده EID 25

در زمان ورود به دستگاه مقصد هر رخداد در دستگاه مقصد منجر به ثبت رویدادی با شناسه EID 4624 خواهد شد. برای مشاهده شواهد اعتبارسنجی انجام شده توسط RDP، در گزارش باید بر روی رویدادهای EID 4624 از نوع Type 10 تمرکز شود.

ID:	4624
Source:	Microsoft Windows security auditing.
Message:	An account was successfully logged on. Subject: Security ID: %1 Account Name: %2 Account Domain: %3 Logon ID: %4 Logon Type: 10 New Logon: Security ID: %6 Account Name: %7 Account Domain: %8 Logon ID: %9 Logon GUID: %10 Process Information: Process ID: %11 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: %13 Source Network Address: %14 Source Port: %15 Detailed Authentication Information: Logon Process: %16 Authentication Package: %17 Transited Services: %18 Package Name (NTLM only): %19 Key Length: %20

شکل ٤ - نمونه‌ای از ساختار رویداد ثبت شده Type 10 در EID 4624

با استفاده از این رویدادهای ثبت شده می‌توان به شواهدی مبنی بر با موفقیت طی شدن مراحل احراز هویت پودمان RDP از یک دستگاه به دستگاه دیگر دست پیدا کرد. این رویدادها اکثرا در یک بستر تجمیع‌کننده[1] نظیر Security Information and Event Management - به اختصار SIEM - ضبط، پردازش و نگهداری شده و توسط ابزارهای جرم‌شناسی رایانه‌ای[2] مورد تجزیه و تحلیل قرار می‌گیرد. در هر دو رویداد ثبت شده EID 21 و EID 25 به نام کاربری و دستگاه مبدا اشاره می‌شود و دستگاه مقصد نیز دستگاهی است که رویداد را ثبت کرده است. باید توجه داشت که در رویداد ذخیره شده و قسمت Source Network Address ممکن است نشانی IP یا نام دستگاه ثبت شده باشد. تحلیلگر اطلاعات می‌تواند برای بررسی دقیق‌تر، از اطلاعات نگاشت میان نشانی IP و نام دستگاه در پودمان DHCP استفاده کند. دانستن اینکه کدام دستگاه به کدام حساب کاربری اختصاص دارد می‌تواند در کسب نتایج مطلوب از تجزیه و تحلیل اطلاعات کمک کند.

شناسایی ناسازگاری‌ها

پس از آنکه شاخص‌های عملکرد فعالیت‌های مرتبط با پودمان RDP در سراسر شبکه از طریق تجزیه و تحلیل رویدادهای ثبت شده مشخص گردید، تحلیلگران امنیتی، شناسایی فعالیت‌های RDP مغایر با قواعد سازمان و الگوهای تایید شده است را آغاز می‌کنند. باید بخاطر داشت که تفکیک فعالیت‌های معتبر و نامعتبر پودمان RDP ممکن است طولانی و زمان‌بر باشد. برای تمایز میان فعالیت‌های مشاهده شده مشکوک و بی‌خطر پودمان RDP می‌توان گزارش رویدادهای ثبت شده سرویس DHCP در نگاشت میان نشانی IP و نام دستگاه را بررسی کرد و یا می‌توان مستندی حاوی نام دستگاه‌ها و نام‌های کاربری به تفکیک واحدهای اداری سازمان تهیه نمود. هر فعالیت پودمان RDP که بر خلاف قواعد تایید شده سازمان انجام شده باید به دقت مورد تحقیق و بررسی قرار گیرد. علاوه بر این، استفاده‌های مجاز از پودمان RDP در صورتی که در مستند مرجع ارتباطات RDP عملکرد وجود نداشته باشد باید به آن اضافه شود تا در تحقیق و تفحص‌های آتی در نظر گرفته شوند.

استفاده از معیارها

با استفاده از روش‌های مرتبط با SIEM، تحلیلگران می‌توانند فعالیت‌های پودمان RDP را براساس نام کاربری، نام دستگاه مبدا و نام دستگاه مقصد دسته‌بندی کنند تا بتوانند تعداد یا مجموع عناصر هر کدام از معیارهای زیر را دقیقا مشخص کنند. کارشناسان امنیت با اطلاع از این معیارها می‌توانند درک دقیق‌تری از فعالیت‌های RDP در داخل شبکه داشته باشند.

- تعیین دستگاه مبدا به ازای هر نام کاربری
- تعیین دستگاه مقصد به ازای هر نام کاربری
- تعیین نام‌های کاربری به ازای هر دستگاه مبدا و مقصد
- تعیین نام‌های کاربری به ازای هر دستگاه مبدا
- تعیین دستگاه‌های مبدا و مقصد به ازای هر نام کاربری
- مجموع تعداد دفعات ورود به دستگاه از طریق پودمان RDP به ازای هر نام کاربری
- مجموع تعداد دفعات ورود به دستگاه از طریق پودمان RDP به ازای هر دستگاه مبدا
- مجموع تعداد دفعات ورود به دستگاه از طریق پودمان RDP به ازای هر دستگاه مقصد
- تعیین دستگاه‌های مبدا به ازای هر دستگاه مقصد
- تعیین دستگاه‌های مقصد به ازای هر دستگاه مبدا

معیارهای مذکور کامل نیستند و موارد دیگری مانند Timestamp Metadata نیز می‌تواند به آنها افزوده شود.

[1] Aggregation Platform
[2] Forensic Computing

توصیه‌ها

هنگام تهیه سند مرجع ارتباطات RDP ممکن است فعالیت افراد تهدیدکننده‌ای که از این پودمان استفاده نمی‌کنند و یا از روش‌های اضافی برای معتبر جلوه دادن فعالیت‌های خود استفاده می‌کنند، به آسانی قابل شناسایی نباشد. اما این سند به تحلیلگران کمک خواهد کرد تا رفتار عادی در محیط شبکه را بهتر درک کرده و ناهنجاری‌ها یا رفتارهای غیرمعتبر را سریع‌تر تشخیص دهند.

رعایت توصیه‌های زیر می‌تواند در به حداکثر رساندن اثربخشی سند مرجع ارتباطات RDP سازمان موثر بوده و در عین حال آسیب‌پذیری سازمان در برابر حملات مبتنی بر پودمان RDP را نیز کاهش دهد.

- از ضدویروس به‌روز و قدرتمند استفاده شود.
- تمامی رمزهای عبور با پیچیدگی قابل قبول تعریف شوند.
- از نصب بودن تمامی اصلاحیه‌های امنیتی اطمینان حاصل شود.
- بجای قابل دسترس کردن دستگاه با نشانی IP عمومی، از پودمان Virtual Private Network - به اختصار VPN - برای اتصال از راه دور کارکنان و پیمانکاران سازمان بهره گرفته شود.
- سیاست Account Lockout Policy در تنظیمات Group Policy فعال شود.
- سرویس Remote Desktop بر روی ایستگاه‌های کاری یا لپ‌تاپ‌ها و به‌طور کلی هر دستگاهی که نیازی به متصل شدن به آنها به‌صورت از راه دور نیست غیرفعال شود.
- ضمن استفاده از دیواره آتش در درگاه شبکه، در دیوار آتش مبتنی بر میزبان[1] نیز قاعده مسدود ساختن ترافیک ورودی پودمان RDP تعریف شود. این امر موجب افزایش محافظت از دستگاه می‌شود. به‌خصوص برای کاربرانی که ممکن است در خارج از سازمان از دستگاه‌های سازمانی استفاده کنند. از قواعد مبتنی بر میزبان زیر می‌توان استفاده کرد:
  * به‌طور پیش‌فرض تمامی ارتباطات ورودی پودمان RDP مسدود شود.
  * در صورت لزوم فقط به نشانی‌های IP تایید شده اجازه برقراری ارتباط RDP داده شود.
- از تنظیم امنیتی Deny log on through Remote Desktop Services برای جلوگیری از اتصال کاربران استاندارد به نقاط پایانی از طریق پودمان RDP استفاده شود.
- از استفاده از پودمان RDP توسط کاربران محلی[2] جلوگیری شود. برای این منظور، اصلاحیه KB2871997 نصب شده و SID زیر به تنظیم Deny log on through Remote Desktop Services افزوده شود:

S-1-5-114: NT AUTHORITY\Local account and member of Administrators group

- اختصاص رمزهای عبور تصادفی برای حساب کاربری Local Administrator با استفاده از راهکار Microsoft LAPS توصیه می‌شود.
- از ثبت گزارش رویدادهای با هر یک از شناسه‌های EID 21، EID 23، EID 24 و EID 25 در بخش Event Log و قسمت TerminalServices LocalSessionManager Operational و ارسال آنها برای راهکار SIEM یا سیستم تجمیع‌کننده رویدادها اطمینان حاصل شود.
- از ثبت گزارش رویداد به شماره شناسه EID 4624 در Event Log و قسمت Security و ارسال گزارش آن به SIEM یا سیستم تجمیع‌کننده رویدادها اطمینان حاصل شود.
- حداکثر اندازه ذخیره‌سازی رویدادها در بخش‌های TerminalServices LocalSessionManager Operational و Event Log به دقت تعیین شود. این تنظیمات را می‌توان از طریق Group Policy Preferences و تغییر مقدار کلید MaxSize در محضرخانه[3] در مسیر زیر انجام داد:

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WINEVT\Channels\Microsoft-Windows-TerminalServices-LocalSessionManager/Operational

[1] Host-based Firewall
[2] Local User
[3] Registry

- حداکثر اندازه ذخیره‌سازی رویدادها در بخش Security به دقت تعیین شود.
- بخش‌های Security و LocalSessionManager Operational و TerminalServices در Event Logs مورد بررسی و نظارت قرار گیرند تا از حذف ناخواسته رویدادها و شواهد جلوگیری شود. (EID 1102)
- ایجاد و به‌روزرسانی منظم اسنادی که در آنها حساب‌های کاربری به تفکیک بخش‌های اداری و نام دستگاه‌های مورد استفاده آنها مشخص شده است.
- از نگهداری شدن رویدادهای پودمان DHCP و دسترسی آسان به آنها اطمینان حاصل شود تا در هر زمان نشانی‌های IP و نام میزبان نگاشت شده در زمان ورود به سیستم قابل شناسایی باشد.

فهرست منابع

- https://www.fireeye.com/blog/threat-research/2018/04/establishing-a-baseline-for-remote-desktop-protocol.html
- https://nakedsecurity.sophos.com/2017/11/15/ransomware-spreading-hackers-sneak-in-through-rdp
- https://www.certcc.ir/news/12389
- https://www.certcc.ir/news/12354
- https://newsroom.shabakeh.net/19430/scarabey.html
- https://newsroom.shabakeh.net/19234/ransomware-spreading-through-rdp.html
- https://github.com/gentilkiwi/mimikatz
- https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/ee891131(v=ws.10)
- https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/ee907364(v%3dws.10)
- https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/ee907330(v%3dws.10)
- https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/ee891126(v%3dws.10)
- https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4624
- https://www.sans.org/summit-archives/file/summit-archive-1498249764.pdf

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. ضدویروس 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

شبکه گستر

شرکت مهندسی شبکه گستر

تهران ۱۹۶۸۶، خیابان شهید دستگردی، شماره ۲۷۳

گروه فروش

داخلی ۱ ۴۲۰۵۲ | sales@shabakeh.net

گروه پشتیبانی

داخلی ۲ ۴۲۰۵۲ | support@shabakeh.net

تارنمای شرکت www.shabakeh.net

خدمات پس از فروش و پشتیبانی my.shabakeh.net

مرکز آموزش events.shabakeh.net

اتاق خبر newsroom.shabakeh.net

شناسه سند: SPT-A-0150-00