هشدارهای IC3 (سازمان شکایت جرایم اینترنتی) درباره حملات پروتکل دسکتاپ از راه دور یا (RDP)

مرکز شکایت جرایم اینترنتی (IC3) در همکاری با وزارت امنیت داخلی ایالات متحده و اف بی آی، هشداری امنیتی را درباره حملات انجام شده از طریق پروتکل دسکتاپ راه دور سیستم عامل ویندوز انجام داده است. در حالیکه بیشتر حملات از طریق پروتکل RDP بیشتر مربوط به باج‌افزارها می‌باشد، مهاجمان از طریق این سرویس، اقدام به سرقت اطلاعات، نصب و راه اندازی درب پشتی و یا به عنوان نقطه شروع برای حملات دیگر استفاده می‌کنند.

این هشدار از US-Cert اعلام کرد:

حملات ابزارهای مدیریت از راه دور، مانند پروتکل دسکتاپ از راه دور (RDP)، از اواسط سال ۲۰۱۶ با افزایش بازارهای سیاه و فروش دسترسیRDP افزایش یافت. مهاجمان سایبری روش‌ها و متودهای شناسایی و بهره‌برداری از نشست‌های آسیب‌پذیر RDP را ابداع کرده‌اند که از طریق اینترنت کارهایی مثل شناسایی هویت افراد، سرقت اطلاعات ورود به سیستم‌ها از جمله نام کاربری و رمز عبور و رمزنگاری اطلاعات حساس برای باج‌گیری را انجام می‌دهد.همچنین توصیه می‌شود که شهروندان چه خصوصی و چه شرکتی بررسی کنند که به شبکه‌های خود چه دسترسی‌هایی از راه دور را اجازه می‌دهند و همچنین اقداماتی را برای کاهش خطرات احتمالی از جمله غیرفعال‌سازی پروتوکل RDP در صورت عدم نیاز به آن، انجام دهند.

همانطورکه اولین بار سال گذشته بازار سیاه و غیرقانونی xDedic ، حساب‌های دارای سرویس دسکتاپ از راه دور هک شده را فقط در ازای ۶ دلار برای هر سرور در فروشگاه خود قرار می‌داد، تا به امروز نیز این کار در بازارهای غیرقانونی ادامه پیدا کرده و سیستم‌های هک شده از طریق سرویس دسکتاپ از راه دور همچنان فروخته می‌شوند.

Windows RDP United Kingdom

Windows RDP United Kingdom Random state in United Kingdom No admin rights Return policy a..

$17.50 Add to Cart
Add to Wish List
Add to Compare

Windows RDP United States

Windows RDP United States Random state in United States No admin rights Return policy ava..

$18.00 Add to Cart
Add to Wish List
Add to Compare

Windows RDP Europe

Windows RDP Europe Random country in Europe No admin rights Return policy available for 3..

$16.00 Add to Cart
Add to Wish List
Add to Compare

Windows RDP Worldwide

Windows RDP Worldwide Random country Worldwide No admin rights Return policy available fo..

~~$14.50~~ **$11.00** Add to Cart
Add to Wish List
Add to Compare

Showing 1 to 12 of 12 (1 Pages)

سایت shodan.io که موتور جستجوی سیستم‌ها ودستگاه‌های متصل به اینترنت است، نشان می‌دهد که درحال حاضر بیش از ۲ میلیون کامپیوتر دارای سرویس دسکتاپ از راه دور وجود دارد که مستقیماً به اینترنت متصل هستند ومنتظرند تا هک شوند.

SHODAN "Remote Desktop Protocol" Explore Downloads Reports Developer Pricing Enterprise Access Contact Us

Exploits Maps Images Share Search Download Results Create Report

TOTAL RESULTS
2,350,134

TOP COUNTRIES

China	551,528
United States	537,209
Germany	105,474
Brazil	100,950
Russian Federation	67,288

TOP SERVICES

RDP	2,321,252
RDP (3388)	28,869
444	5
Webmin	3
9002	1

Telebucaramanga S.A. E.s.p.
Added on 2018-09-28 18:45:38 GMT
Colombia
Details
self-signed

SSL Certificate
Issued By:
|- Common Name:
Issued To:
|- Common Name:
Supported SSL Versions
TLSv1, TLSv1.1, TLSv1.2
Diffie-Hellman Parameters
Fingerprint: RFC2409/Oakley Group 2

Remote Desktop Protocol
\x03\x00\x00\x0b\x06\xd0\x00\x00\x124\x00

Videotron Ltee
Added on 2018-09-28 18:45:36 GMT
Canada, Vaudreuil
Details
self-signed

SSL Certificate
Issued By:
|- Common Name: Serveur-PC
Issued To:
|- Common Name: Serveur-PC
Supported SSL Versions
TLSv1, TLSv1.1, TLSv1.2

Remote Desktop Protocol
\x03\x00\x00\x0b\x06\xd0\x00\x00\x124\x00

همچنین درباره اینکه چگونه آلودگی‌های باج‌افزاری مانند CrySiS/Dharma ، SamSam ، BitPaymer و CryptON چگونه از طریق پروتوکل دسکتاپ از راه دور کل سیستم‌ها را آلوده می‌کنند، تحقیقات زیادی انجام شده است.

از آنجا که این حملات، کل شبکه را به جای یک کامپیوتر هدف قرار می‌دهند و قیمت‌هایی از ۳۰۰۰ تا ۵۰۰۰ دلار را برای یک کامپیوتر تکی و نزدیک به ۵۰۰۰۰ دلار و بیشتر را برای رمزگشایی کل شبکه درخواست می‌کنند، پس باید این موضوع به سرعت عمومی‌سازی شود و به اطلاع همه مردم برسد.

به عنوان مثال حملات به شرکت ورزشی آمریکایی PGA در بندر آتلانتا و سان‌دیگو و همچنین تعداد زیادی بیمارستان از طریق این پروتوکل دسکتاپ از راه دور که سیستم‌ها را در معرض دسترسی اینترنتی قرار می‌دهد، انجام شد.

پس خیلی مهم است که همه سازمان‌ها و نهادهایی که به این پروتوکل مجهز هستند، از این سرویس خود نهایت محافظت را به عمل آورند.

محافظت از پروتکل دسکتاپ از راه دور یا RDP

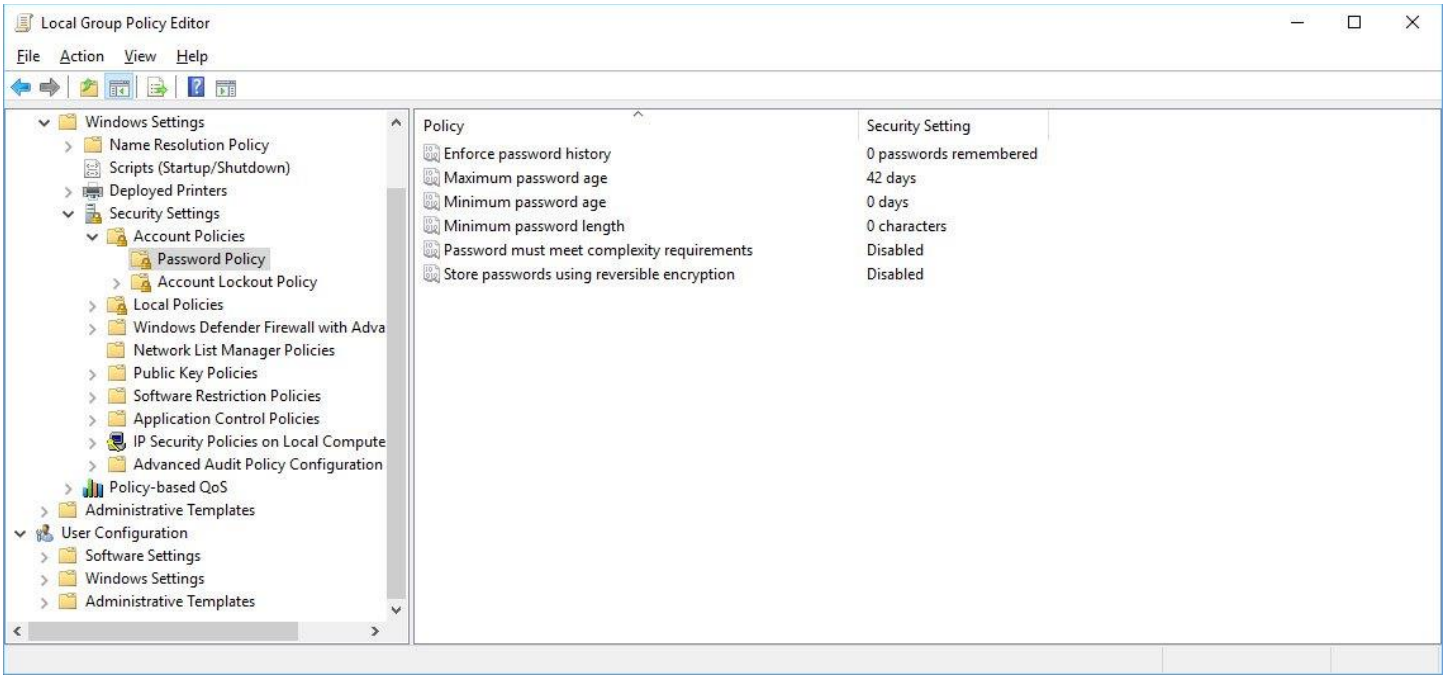
استفاده از پروتوکل و سرویس دسکتاپ از راه دور یک کار جدایی ناپذیر برای استفاده از منابع در شرکت‌ها وسازمان‌هاست و گفته نمی‌شود که حتما باید آن را غیرفعال کنید، بلکه پیشنهاد می‌شود که باید از آن به درستی محافظت شود.

در زیر مراحل مختلفی برای محافظت از این سرویس مشخص شده است:

۱. هیچوقت سرویس دسکتاپ از راه دور خود را مستقیما به اینترنت متصل نکنید : به جای اتصال مستقیم این سرویس به اینترنت، شرکت‌ها می‌توانند این سرویس را پشت یک دیواره آتش یا VPN قرار دهند تا فقط افراد مجاز توانایی دسترسی به این سرویس را داشته باشند. انجام این کار موجب سخت‌تر شدن پیدا کردن سرورهای آسیب‌پذیر و انجام حملات جستجوی فراگیر فضای کلید (brute force) برای دسترسی به رمز عبور می‌شود.

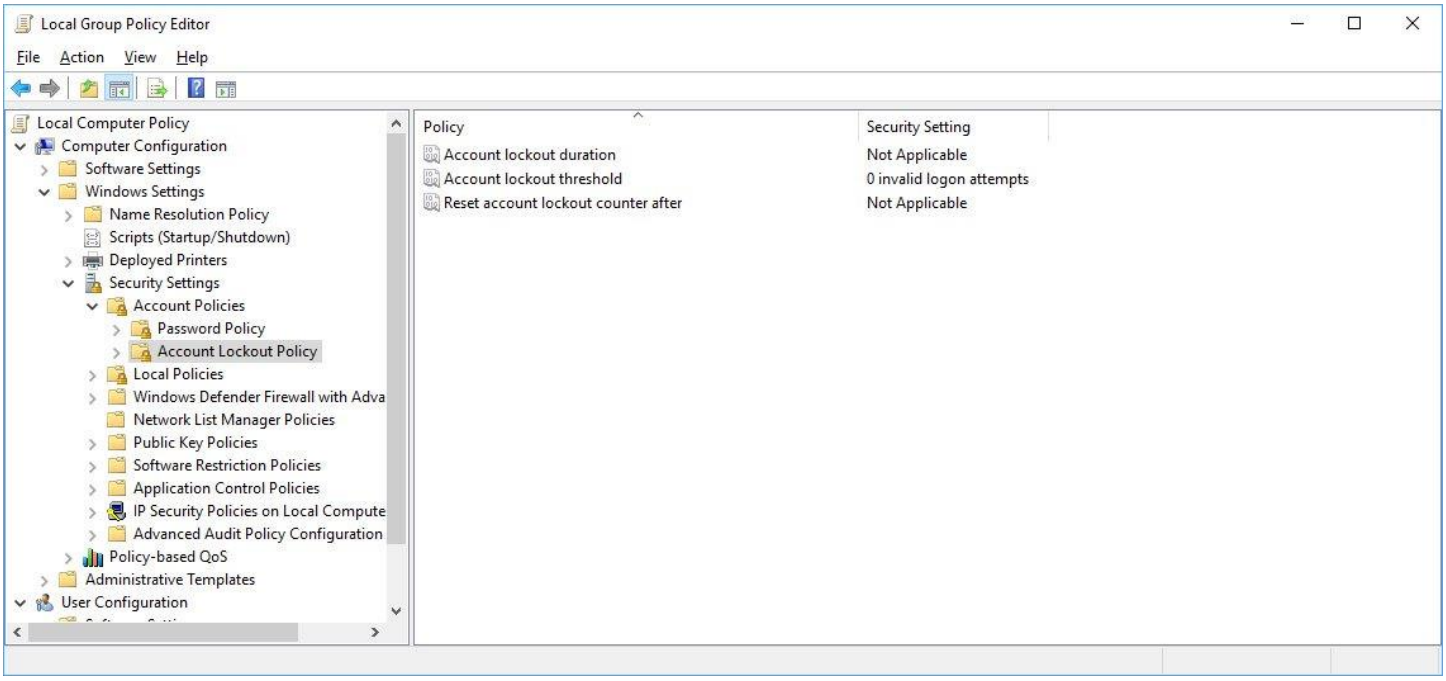
همچنین اگر می‌توانید پورت TCP پروتوکل دسکتاپ از راه دور خود را از حالت پیشفرض ۳۳۸۹ به یک مقدار غیر استاندارد تغییر دهید. این کارکه یکی از متودهای محافظتی است، مقداری به امنیت سرویس شما کمک می‌کند وآن را امن‌تر می‌کند.

۲. از رمز عبورهای قوی و اعتبارسنجی‌های چند فاکتوره استفاده کنید: مهاجمان سرویس دسکتاپ از راه دور از روش جستجوی فراگیر فضای کلید (brute force) استفاده می‌کنند و رمزعبور درست را حدس می‌زنند. پس خیلی مهم است که از رمزعبورهای سخت وپیچیده استفاده کنید وبرای این کار می‌توانید به سیاست‌های رمزعبور قوی ویندوز مراجعه کرد.

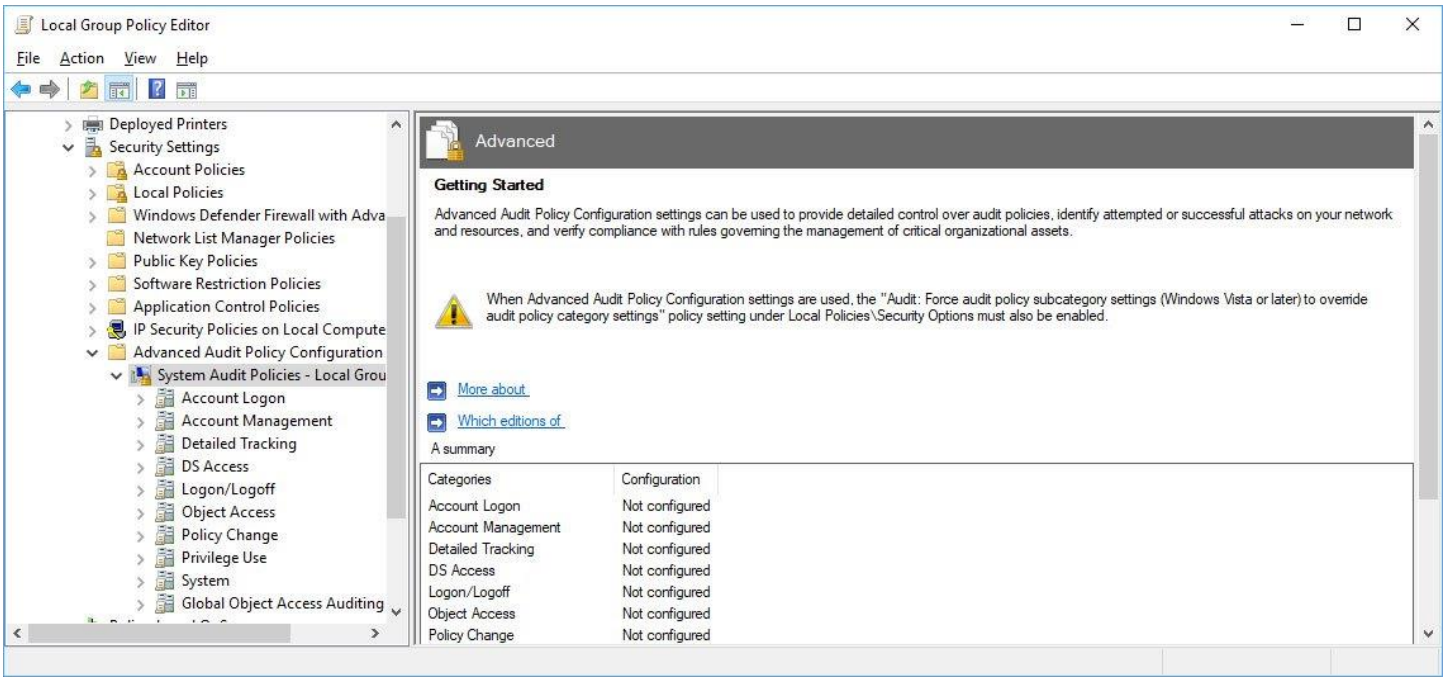


برای امنیت بیشتر، بعضی شرکت‌ها از اعتبارسنجی‌های چند فاکتوره هم استفاده می‌کنند.

۳. سیاست‌های قفل حساب را فعال کنید: فعال کردن این ویژگی موجب می‌شود که مهاجمان بعد از چند بار تلاش برای امتحان کردن رمزهای عبور ناموفق به صورت موقت نتوانند وارد سیستم شوند که این ویژگی کار را برای آنها سخت‌تر می‌کند، زیرا حملات جستجوی فراگیر فضای کلید (brute force) به تلاش‌های متعدد وتکراری برای وارد کردن رمزعبور بستگی دارد که با این ویژگی مسدود می‌شود.



۴. فعالسازی حسابرسی و ثبت ورود به حساب‌ها: با فعال کردن این ویژگی مدیران حساب‌ها میتوانند مشاهده کنند که چه حساب‌هایی چندبار متعدد رمزعبور را اشتباه وارد کرده‌اند و از این طریق این حساب‌های مشکوک را شناسایی کرد.



۵. بروزرسانی‌های امنیتی را فوراً نصب کنید: و در انتها بروزسانی و آپدیت‌ها را حتماً فراموش نکنید. می‌دانیم که برای خیلی از شرکت‌ها خیلی سخت است که بلافاصله بروزرسانی‌ها را نصب کنند ولی پیشنهاد ما این است که در اسرع وقت این بروزرسانی‌ها را نصب کنید تا سیستمتان امن بماند.