禪

کاربران مراقب باشند

باجافزارها از طریق پروتکل ریموت دسکتاپ RDP حمله میکنند

مدیران شبکههایی که از ریموت دسکتاپ ویندوز برای اتصال به ایستگاههای کاری از خارج مجموعه استفاده میکنند، در معرض حملات باجافزارها هستند . به تازگی نمونههایی از باجافزارها کشف شدهاند که از طریق ضعف امنیتی ریموت دسکتاپ ویندوز اقدام به ورود به سیستم و کدگذاری فایلها میکنند و پس از آن مبالغ هنگفتی را برای بازگرداندن اطلاعات طلب میکنند .

چگونگی عملکرد این باج افزارها بدین صورت است که ابتدا باجگیران از طریق نرمافزارهای خودکار اقدام به اسکن درگاههای باز روی آدرسهای IP اینترنتی کرده و در صورتی که پورت ریموت دسکتاپ روی آنها باز باشد، اقدام به حدس زدن رمزهای عبور مختلف نموده و شانس خود را برای ورود به سیستم محک میزنند . در صورتی که فایروالی با قابلیت تشخیص اینگونه حملات روی لبه شبکه فعال نباشد و همچنین مقرراتی برای جلوگیری از ورود پسوردهای اشتباه به دفعات متعدد موجود نباشد، ممکن است بعد از گذشت فاصله زمانی کمی، نرمافزارهای باجگیر بتوانند رمز عبور صحیح را حدس زده و دسترسی ورود به سیستم را دریافت کنند .

vmware
Keyboard and Mouse
RDP TCP/IP
Client
Terminal Server
Keyboard and Mouse

1-

2- [illegible] P@ssw0rd [illegible].

3- [illegible] IPS/IDS [illegible].

4- [illegible] IP [illegible] IP [illegible] 3389 [illegible].

5- [illegible].

6- [illegible].

7- [illegible].

8- [illegible].

[illegible]:
[illegible]
[illegible]:
[illegible]
[illegible]:
[illegible]
[illegible]:
16:16 - 27/10/1395
[illegible]:
[illegible] - [illegible] - [illegible] - [illegible] - [illegible] - [illegible]

[illegible]: https://www.shabakeh-mag.com/security/6403