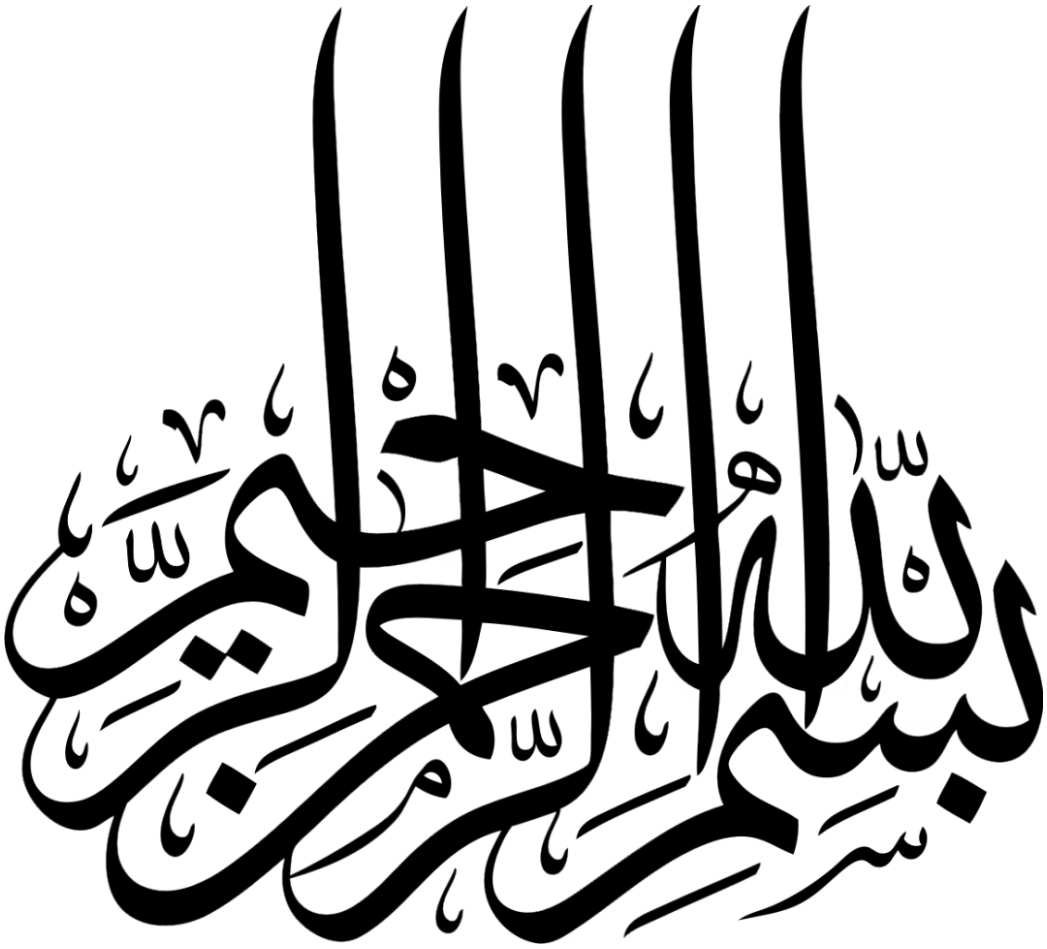

بسم الله الرحمن الرحیم

Ransomware Again But We Changed the RDP Port

تهیه شده توسط تیم تولید محتوای وب سایت چلنجینو

فهرست مطالب

مقدمه

در این مقاله با یک واقعیت مهم در امنیت مواجهیم: تغییر پورت RDP به‌تنهایی هیچ تضمینی برای امن‌بودن نیست.

مهاجمان امروزی صرفاً پورت پیش‌فرض ۳۳۸۹ را هدف نمی‌گیرند؛ آن‌ها با اسکن گسترده و حملات Brute Force، سرویس RDP را روی پورت‌های غیراستاندارد هم پیدا می‌کنند و در صورت دستیابی به یک حساب معتبر، خیلی سریع زنجیره حمله را ادامه می‌دهند.

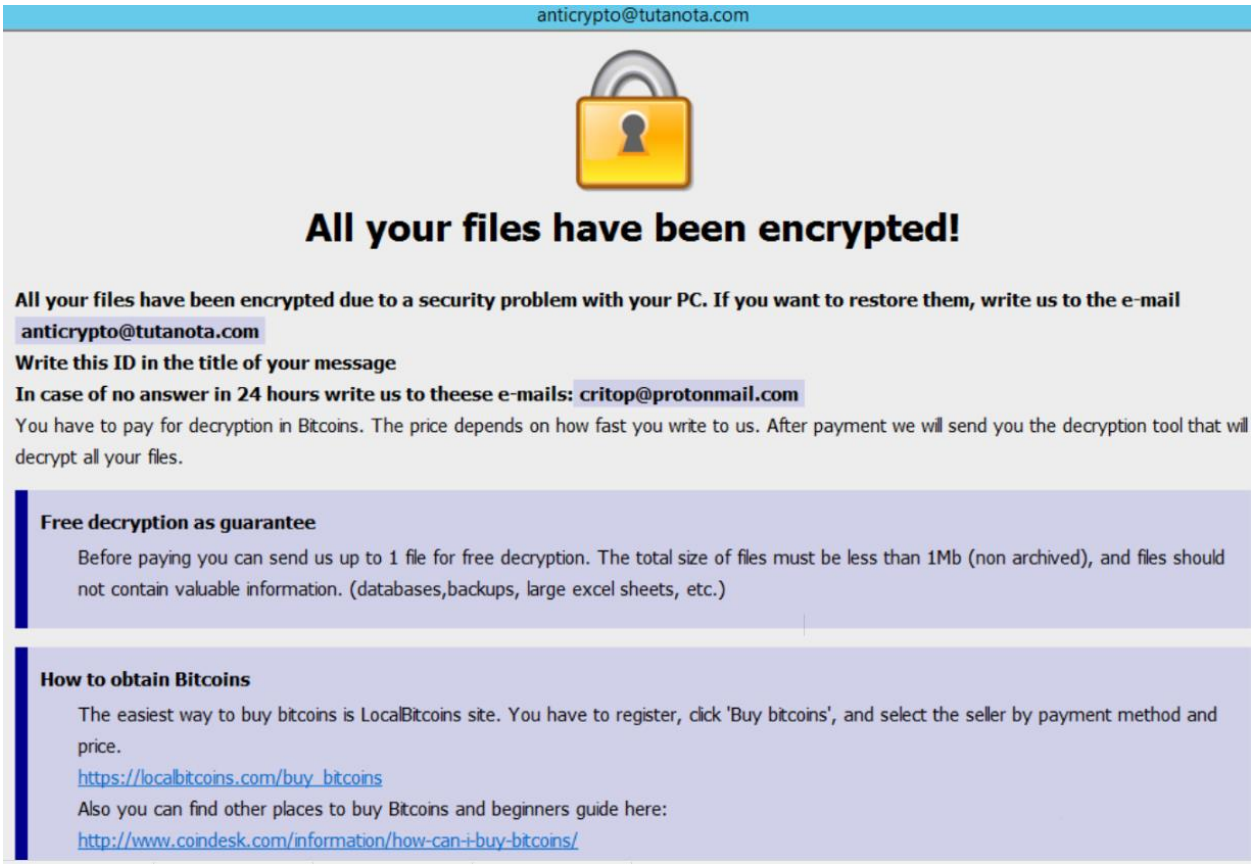
گزارشی که در ادامه می‌آید نمونه‌ای واقعی از همین مسئله است؛ جایی که مهاجم پس از ورود از طریق RDP، در چند دقیقه با ابزارهای شناسایی شبکه محیط را بررسی کرده، سپس به Domain Controller متصل شده و در کمتر از حدود ۱۷ دقیقه باجافزار Harma (از خانواده Dharma/CrySiS) را روی دو سیستم اجرا کرده است.

این مطالعه موردی نشان می‌دهد چرا اتکا به پنهان‌سازی سرویس‌ها کافی نیست و چرا باید کنترل‌های جدی‌تری مثل غیرفعال‌سازی حساب‌های پیش‌فرض، استفاده از MFA، محدودسازی دسترسی‌ها و ترجیحاً قرار دادن RDP پشت VPN یا راهکارهای واسط امن را به‌کار گرفت.

مطالعه این گزارش می‌تواند دید بهتری نسبت به رفتار مهاجمان، ابزارهای مورد استفاده و تکنیک‌های به‌کاررفته در چنین حملاتی ارائه دهد و به درک بهتر نحوه شناسایی و مقابله با این تهدیدات کمک کند.

توضیحات اولیه

با مثال دیگری از حمله باج‌افزاری از طریق Brute Force RDP در خدمت شما هستیم.



این بار سیستمی که Brute Force شد از پورت پیش‌فرض RDP استفاده نمی‌کرد. مهاجمان توانستند باج‌افزار را روی دو ماشین، که شامل یک Domain Controller بود، در حدود ۱۷ دقیقه نصب کنند.

یک توییت اخیراً گفته بود: «فقط پورت RDP را تغییر بده و امن هستی».

ما کاملاً با این نظر مخالفیم.

جدول زمانی رخدادها (UTC):

۰۷:۰۰ – ورود RDP از آی‌پی ۲۱۲.۱۰۲.۴۵.۹۸

۰۷:۰۱ – باز کردن Task Manager (معمولاً برای دیدن اینکه چه کسانی دیگر وارد سیستم شده‌اند)

۰۷:۰۳ – اجرا / قرار دادن Network Scanner

۰۷:۰۸ – RDP به یک Domain Controller

۰۷:۱۰ – در DC: باز کردن Task Manager

۰۷:۱۰ – در DC: اجرا/ قرار دادن Network Scanner

۰۷:۱۳ – در DC: قرار دادن باج‌افزار Harma روی دسکتاپ و اجرای آن

۰۷:۱۷ – در نقطه ورود: قرار دادن باج‌افزار Harma روی دسکتاپ و اجرای آن

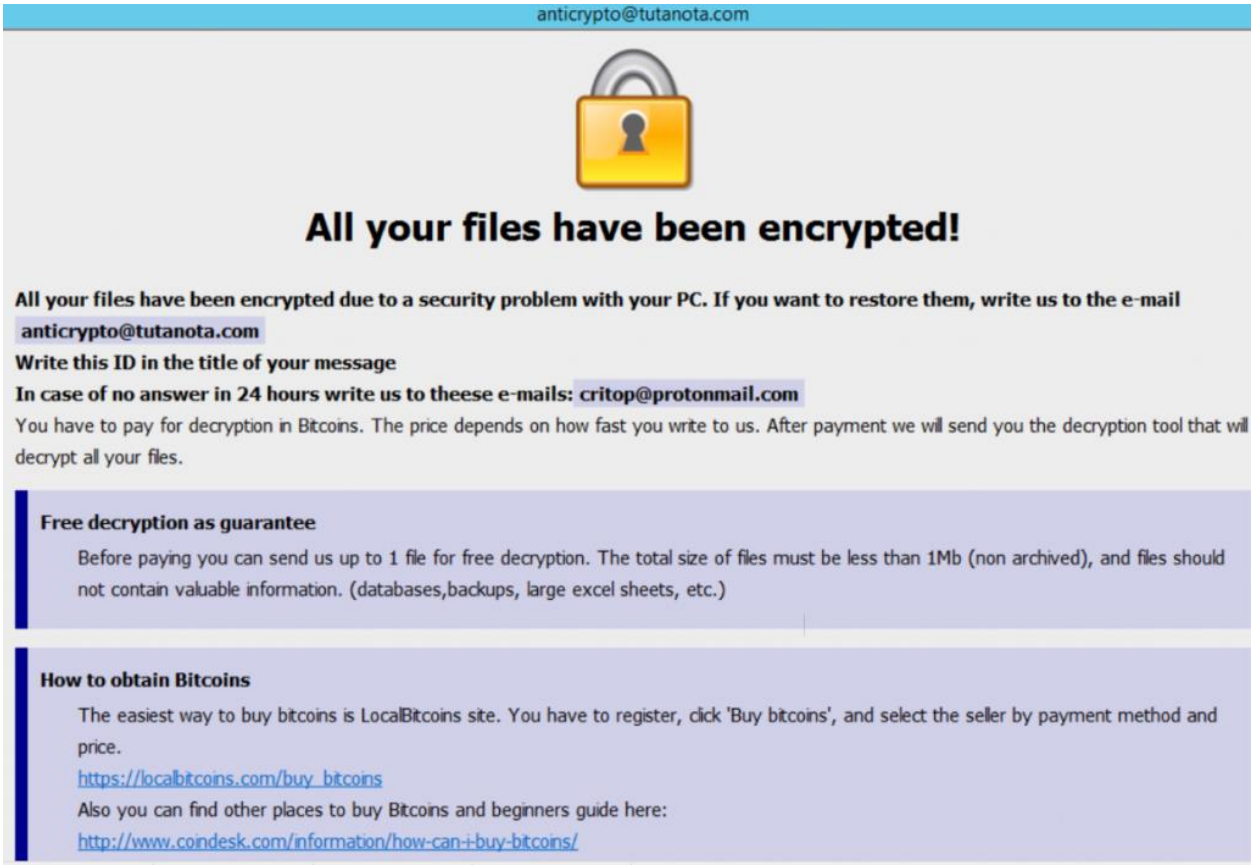
Harma

Harma یک نوع (variant) از Dharma/CrySiS است که قبلاً در گزارش های دیگر در سایت The DFIR Report درباره آن نوشته شده است.

این دو باج‌افزار شباهت‌های زیادی دارند، از جمله مسیر مشترک PDB.

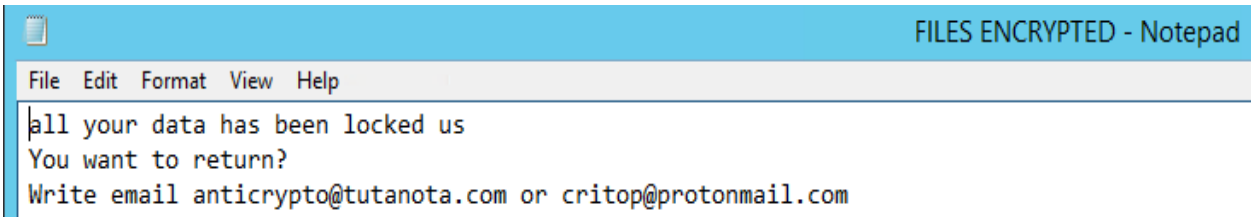
debugger-stamp	0x58B8AF72 (Thu Mar 02 23:49:06 2017)
path	c:\crysis\release\pdb\payload.pdb
guid	906D7E25-96FC-4243-8EC3-87236B61A492

یادداشت‌های باج‌افزار هم شباهت زیادی به هم دارند.




```
"A service was installed in the system.

Service Name:  bizkaz
Service File Name:  cmd.exe /c echo bizkaz > \\.\pipe\bizkaz
Service Type:  user mode service
Service Start Type:  demand start
Service Account:  LocalSystem"
```



خلاصه

تغییر پورت RDP مانع فعالیت مهاجمان نمی‌شود. ما به طور مداوم برای پروتکل RDP تقریباً روی همه پورت‌هایی که باز می‌کنیم، اسکن می‌شویم.

اگر مجبورید RDP را از طریق اینترنت استفاده کنید به موارد زیر توجه نمایید:

- حساب‌های پیش‌فرض را غیرفعال کنید.
- از MFA (احراز هویت چندمرحله‌ای) استفاده کنید.

با این حال، همچنان توصیه می‌کنیم از VPN یا یک واسطه مثل VMware View یا Citrix Workspace همراه با MFA استفاده نمایید.

IOSها (Indicators of Compromise)

MISP Priv 69099 / 21ce5f26-43bb-4971-a02d-59b563c4e3ca

ورود RDP از آی‌پی: ۲۱۲.۱۰۲.۴۵.۹۸

BPY6A7_payload.exe

56452e0839ef830c904182992aa11691

e94e21979565c2372fc2745f18eec3c64d9cc2da

23a3dfe1493dcda00a3d9a00210793553b629bd77f30c39974c8e1ab0ea51c6f

5-NS new.exe

597de376b1f80c06d501415dd973dcec

629c9649ced38fd815124221b80c9d9c59a85e74

f47e3555461472f23ab4766e4d5b6f6fd260e335a6abc31b860e569a720a5446

Persistence

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp\BPY6A7_payload.exe

MITRE ATT&CK

- External Remote Services - T1133
- Network Share Discovery - T1135
- Data Encrypted for Impact - T1486
- Valid Accounts - T1078
- Internal case 1001

منبع:

https://thedfirreport.com/2020/07/13/ransomware-again-but-we-changed-the-rdp-port/