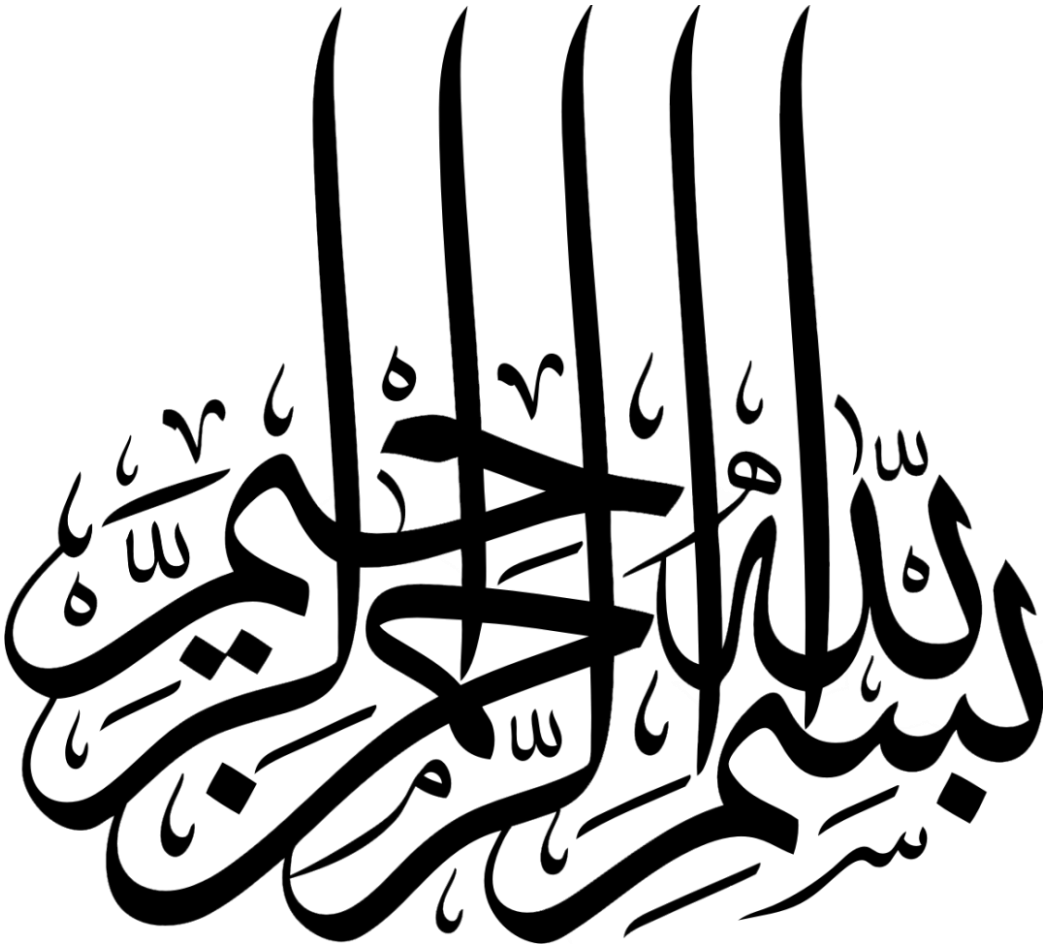

بسم الله الرحمن الرحیم

Dharma Ransomware

تهیه شده توسط تیم تولید محتوای وب سایت چلنجینو

فهرست مطالب

مقدمه

در سال‌های اخیر، باج‌افزارها به یکی از جدی‌ترین تهدیدهای امنیتی در سازمان‌ها تبدیل شده‌اند؛ حملاتی که اغلب نه با تکنیک‌های پیچیده، بلکه با سوءاستفاده از ضعف‌های رایج مثل دسترسی ناامن RDP، رمزهای عبور ضعیف و نبود نظارت کافی آغاز می‌شوند.

در این گزارش، یک نمونه واقعی از حمله باج‌افزار Dharma بررسی شده است؛ حمله‌ای که نشان می‌دهد چگونه یک نفوذگر می‌تواند تنها در چند دقیقه، از طریق دسترسی از راه دور (RDP) وارد شبکه شود، سطح دسترسی خود را از مدیر محلی به مدیر دامنه ارتقا دهد و در نهایت باج‌افزار را روی چندین سیستم اجرا کند.

اهمیت این گزارش در آن است که به‌خوبی روند سریع و خطرناک یک نفوذ را نشان می‌دهد؛ جایی که تنها چند تصمیم نادرست امنیتی مثل فعال‌بودن RDP بدون محدودیت یا نبود نظارت آنی می‌تواند امنیت کل شبکه را به خطر بیندازد. مطالعه‌ی این مورد کمک می‌کند تا تیم‌های امنیتی و مدیران فناوری اطلاعات درک بهتری از مراحل واقعی نفوذ و روش‌های جلوگیری از آن پیدا کنند.

توضیحات اولیه

یک مهاجم از طریق RDP به honeypot با آی‌پی 178.239.173[.]172 وارد شد.

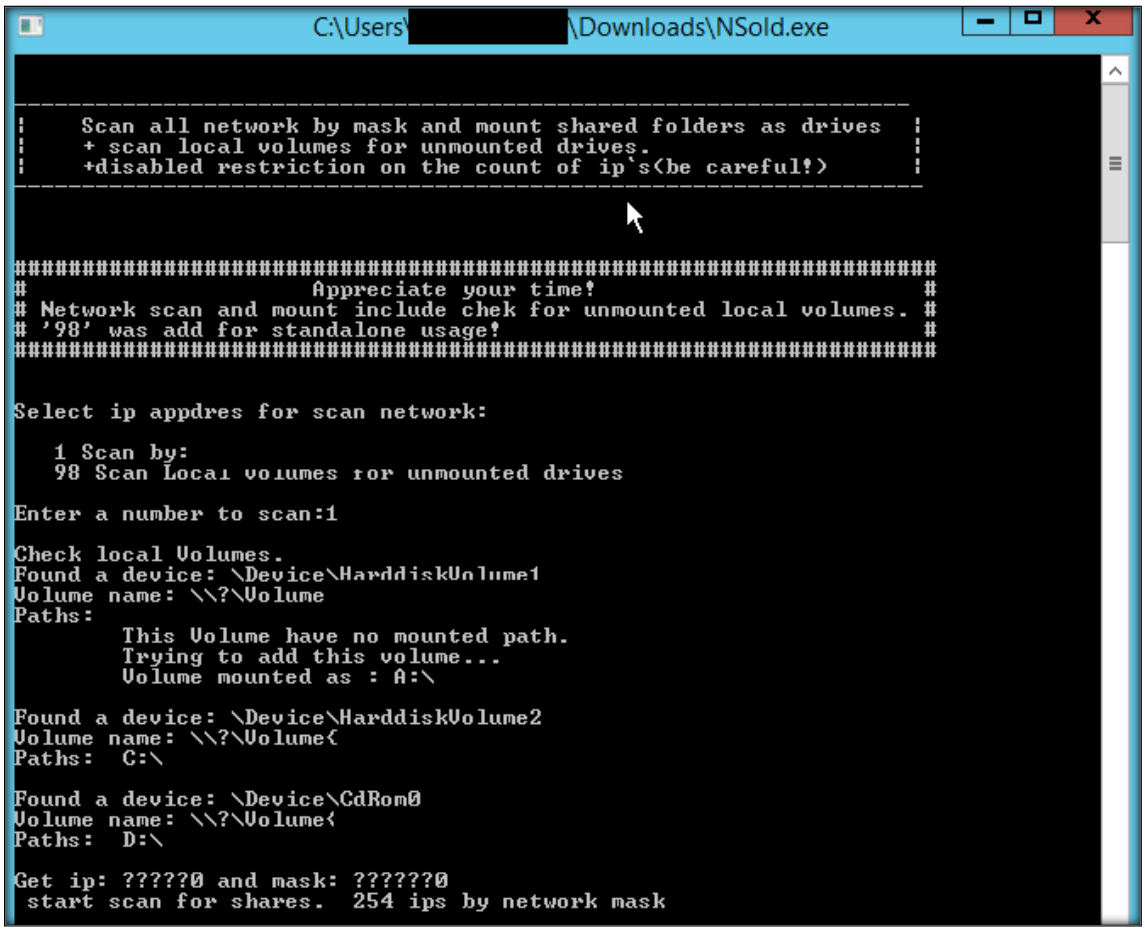
در ۱۰ دقیقه، مهاجم توانست از مدیر محلی (local admin) به مدیر دامنه (domain admin) ارتقا یابد و سپس باج‌افزار را روی چندین سیستم نصب کند.

مهاجم ابتدا از Defender Control استفاده کرد تا Defender ویندوز را خاموش کند و سپس از Mimikatz برای استخراج رمزهای عبور استفاده کرد.

بعد از آن، مهاجم از Network Scanner برای اسکن شبکه محلی (local subnet) استفاده کرد.

سپس مهاجم با RDP به هر سیستم متصل شد تا باج‌افزار را به صورت دستی اجرا کند.

این یک تصویر از Network Scanner است که توسط مهاجمان به NSold.exe تغییر نام داده شد.



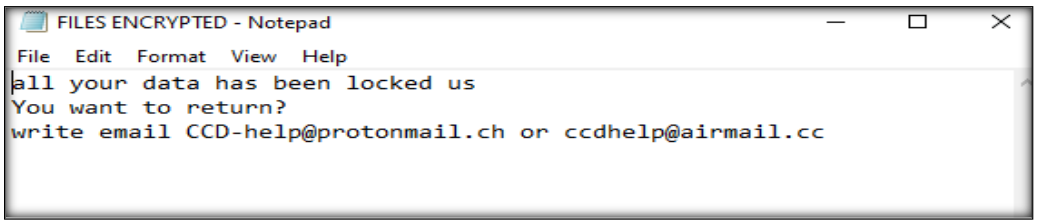
لاگ‌های زیر، استخراج و استفاده از DefenderControl برای غیرفعال کردن Windows Defender در طول حمله را نشان می‌دهند:

data.win.eventdata.image	data.win.eventdata.commandLine	rule.description
C:\\Users\\[redacted]\\Downloads\\DefenderControl.exe	-	[redacted]
C:\\Users\\[redacted]\\Downloads\\DefenderControl.exe	-	[redacted]
C:\\Users\\[redacted]\\Downloads\\DefenderControl.exe	-	[redacted]
C:\\ProgramData\\Microsoft\\Windows Defender\\Platform\\4.18.2003.8-0\\MpCmdRun.exe	\"C:\\ProgramData\\Microsoft\\Windows Defender\\platform\\4.18.2003.8-0\\MpCmdRun.exe\" -DisableService	MITRE T1089 Disabling Security Tools: C:\\ProgramData\\Microsoft\\Windows Defender\\Platform\\4.18.2003.8-0\\MpCmdRun.exe
C:\\ProgramData\\Microsoft\\Windows Defender\\Platform\\4.18.2003.8-0\\MpCmdRun.exe	\"C:\\ProgramData\\Microsoft\\Windows Defender\\platform\\4.18.2003.8-0\\MpCmdRun.exe\" -DisableService	MITRE T1089 Disabling Security Tools: C:\\ProgramData\\Microsoft\\Windows Defender\\Platform\\4.18.2003.8-0\\MpCmdRun.exe
-	-	Windows Defender: Realtime Detection Disabled: https://attack.mitre.org/techniques/T1089/

این یک اسکرین‌شات از یادداشت باج (ransom note) است که در زمان ورود به سیستم ظاهر می‌شود.

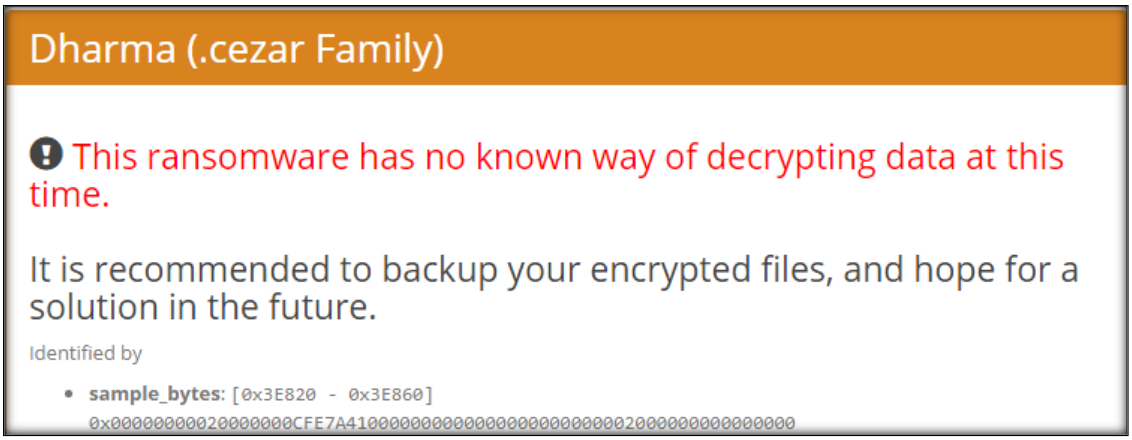
این فایل FILES ENCRYPTED را می‌توان در root درایو C و همچنین روی دسکتاپ پیدا کرد.

به نظر می‌رسد این فایل در هر پوشه‌ای که رمزگذاری اتفاق افتاده است نوشته شده است.



ما این دستور را چندین بار در نفوذهای باجافزاری دیده‌ایم و ممکن است ارزش داشته باشد که یک قانون برای شناسایی findstr.exe با پارامترهای $/c:system و یا $/c:sistem در آرگومان‌های خط فرمان نوشته شود.

ما اطلاعات را به ID Ransomware ارسال کردیم که اطلاعات زیر را ارائه داد:



ما همین مسیر pdb را در گذشته برای Dharma دیده‌ایم، بنابراین این مسیر ثابت می‌ماند و می‌تواند یک روش خوب برای شناسایی باشد.

جهت اطلاعات بیشتر می‌توانید به لینک زیر مراجعه نمایید:

https://id-ransomware.blogspot.com/2016/11/dharma-ransomware.html

خلاصه:

این مهاجم توانست باج‌افزار را روی ۵ سیستم و یا بیشتر از آن، در کمتر از ۱۰ دقیقه نصب کند که واقعاً چشمگیر بود.

مهاجم از Defender Control استفاده کرد که قبلاً هم دیده بودیم تا Defender ویندوز را غیرفعال کند و از Mimikatz برای استخراج رمزهای عبور استفاده کرد.

می‌توان چندین قانون شناسایی (detection rules) از این نفوذ نوشت که به بهبود زمان شناسایی در آینده کمک می‌کند.

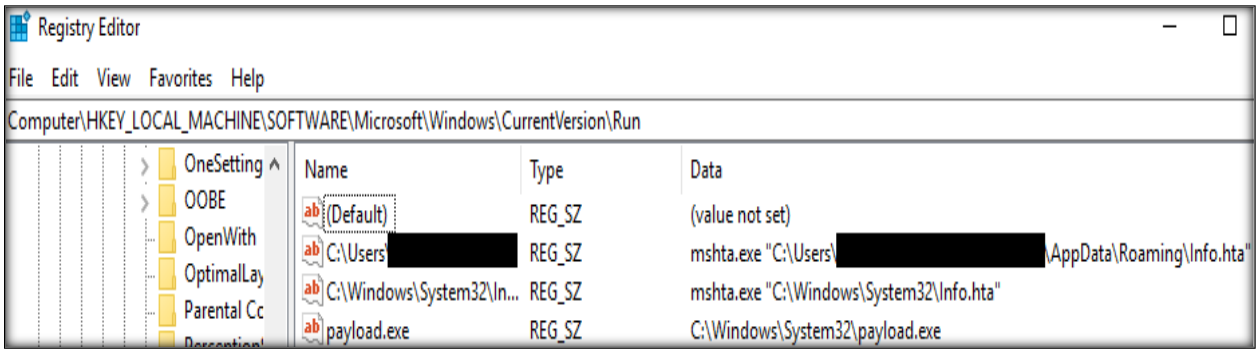
با این حال، وقتی مهاجمان اینقدر سریع حرکت می‌کنند، باید به موقع به حادثه‌ها پاسخ داد تا مهاجم قبل از انجام مأموریتش متوقف شود.

IOCs

ransomware payload که بخشی از باج‌افزار که فایل‌ها را رمزگذاری می‌کند یا عمل اصلی حمله را انجام می‌دهد، می تواند توسط Any.Run که سرویس آنلاین برای تحلیل رفتار بدافزارهاست، شناسایی شود.

ورود از طریق پروتکل RDP

کلیدهای رجیستری که باعث اجرای برنامه‌ها هنگام شروع ویندوز می‌شوند در تصویر زیر قابل مشاهده می‌باشند:



منبع:

https://thedfirreport.com/2020/04/14/dharma-ransomware/