NCSC VN
National Cyber Security Center

Trung tâm Giám sát an toàn không gian mạng quốc gia

BÁO CÁO

Phân tích về Ransomware LockBit 3.0

Phần I: Ransomware LockBit 3.0

Băng nhóm ransomware LockBit là một trong những nhóm ransomware nguy hiểm hàng đầu trên thế giới. Kể từ khi xuất hiện lần đầu tiên vào năm 2019, LockBit đã tổ chức nhiều cuộc tấn công nhắm vào các tổ chức trên nhiều lĩnh vực khác nhau, LockBit hoạt động dưới dạng Ransomware-as-a-Service (RaaS), cho phép các tác nhân đe dọa triển khai ransomware và chia sẻ lợi nhuận với những kẻ đứng sau dịch vụ ransomware.

Các phiên bản LockBit

Ransomware LockBit lần đầu được biết đến với tên "ABCD" (được đặt theo tên phần mở rộng tệp bị mã hóa), và sau vài tháng biến thể của "ABCD" xuất hiện với cái tên như hiện tại "LockBit". Một năm sau, nhóm này đã phát hành phiên bản nâng cấp của ransomware có tên "LockBit 2.0" (hoặc "LockBit Red"), bao gồm một phần mềm độc hại tích hợp khác có tên là "StealBit" với mục đích đánh cắp dữ liệu nhạy cảm.

Phiên bản mới nhất hiện tại là "LockBit 3.0" (hay "LockBit Black"), xuất hiện vào năm 2022 với các tính năng mới và các kỹ thuật né tránh bảo mật nâng cao.

Vào tháng 9 năm 2022, mã nguồn của LockBit 3.0 đã bị rò rỉ bởi một đối tượng có bí danh "ali_qushji" trên nền tảng X (trước đây là Twitter). Vụ rò rỉ bao gồm một số tệp có thể được sử dụng để phát triển ransomware này. Vụ rò rỉ này cho phép các chuyên gia phân tích kỹ hơn về mẫu ransomware này và cũng từ đó các tác nhân đe dọa đã tạo ra một làn sóng các biến thể ransomware mới, dựa trên mã nguồn của LockBit 3.0.

Phần II: Các cụm LockBit đang hoạt động

"TronBit"

TronBit thường kết nối đến mục tiêu thông qua TeamViewer. Thông tin kết nối thường được thu thập từ thông tin đăng nhập bị rò rỉ hoặc những thông tin có được thông qua việc triển khai mã độc đánh cắp thông tin

Khi thực thi tệp .exe của LockBit 3.0, mã độc tắt Windows Defender, hình nền màn hình sẽ chuyển sang màn hình đen với một thông báo cho biết cuộc tấn công ransomware đã xảy ra và hướng dẫn người dùng xem thông báo tiền chuộc được lưu trong mỗi thư mục tại tệp ID.README.txt. Ngoài ra, một số biểu tượng tệp được thay thế bằng biểu tượng LockBit 3.0. Thông báo đòi tiền chuộc thường hiển thị như sau:

```
                >>>> Your data are stolen and encrypted

      if you do not pay the ransom The Your data permanently deleted

>>>>What guarantees that we will not deceive you?

      We are not a politically motivated group and we do not need anything
other than your money.
      If you pay, we will provide you the programs for decryption and your
data will not be disclosed .
      Life is too short to be sad. Be not sad, money, it is only paper.
    You can contact us and use your personal decryption ID to decrypt a
file for free
>>>>Your personal DECRYPTION ID: [ID]
      If we do not give you decrypters after payment, then nobody will pay
us in the future.
      Therefore, our reputation is very important to us.

>>>>Pay ransom amount 1000$
>>>>Payment cryptocurrency address USDT-TRC20
>>>>[USDT-TRC20 ADDRESS]
>>>>payment is completed, send the payment photo to Email:    [EMAIL
ADRESS]
>>>>payment is completed Send via email we will provide you the programs
      You can contact me by email.
      Email:[EMAIL ADRESS]
```

Các mẫu địa chỉ email sau đây đã từng xuất hiện trong thông báo đòi tiền chuộc:

- spiroshalkis[@]mail.com
- ericducke[@]mail.com
- contactbit8cca[@]proton.me
- tpichughinn[@]mail.com
- donahuerolland[@]proton.me

Nạn nhân của TronBit trải rộng trên nhiều lĩnh vực trên toàn cầu, tuy nhiên, trọng tâm của các cuộc tấn công này có xu hướng chủ yếu nhắm vào các doanh nghiệp SMB (doanh nghiệp vừa và nhỏ).

Phần II: Các cụm LockBit đang hoạt động

"CriptomanGizmo"

Một số tấn công LockBit 3.0 được thực hiện bởi một đối tượng có tên là "CriptomanGizmo". Các cuộc tấn công này đặc biệt nhắm vào các cá nhân hoặc tổ chức tương đối "nhỏ", thường là các máy tính cá nhân và doanh nghiệp nhỏ. CriptomanGizmo trước đây đã sử dụng nhiều chủng ransomware khác nhau, bao gồm cả STOP/DJVU.

Điểm xâm nhập ban đầu được cho là thông qua các giao thức truy cập máy tính từ xa (RDP). Các thông tin RDP có thể bắt nguồn từ việc thông tin xác thực bị rò rỉ, mật khẩu yếu hoặc máy chủ RDP kết nối với Internet được cấu hình không an toàn cho phép những tác nhân độc hại kết nối từ xa. Ví dụ về thông báo đòi tiền chuộc trong cuộc tấn công ransomware CriptomanGizmo:

```
                    YOUR FILES ARE ENCRYPTED!!!
For data recovery contact us you will need to pay us:
returnback[@]cyberfear.com
returnbac[@]onionmail.org
@returnbacc
https://t[.]me/returnbacc
1. In the first letter, indicate your personal ID!
2. In response, we will send you instructions.

>>>> Your personal DECRYPTION ID: [ID]
```

Các mẫu địa chỉ email được tìm thấy trong thông báo đòi tiền chuộc trong các cuộc tấn công của CriptomanGizmo:

returnback[@]cyberfear.com	Email address
returnbac[@]onionmail.org	Email address
warthunder089[@]mailfence.com	Email address
warthunder089[@]tutanota.de	Email address
help_havaneza[@]cryptolab.net	Email address
help_havaneza[@]bastardi.net	Email address
mrbrook[@]msgsafe.io	Email address
fireco[@]onionmail.com	Email address
firecorecoverfiles[@]msgsafe.io	Email address
@firecorecoverfiles	Telegram indicator
carabas1337[@]proton.me	Email address
fiileky2023[@]onionmail.com	Email address

Phần II: Các cụm LockBit đang hoạt động

"Tina Turner"

Đây là cụm ransomware thường tấn công và tiến hành in hàng loạt thông báo đòi tiền chuộc trên mọi mọi thiết bị in được kết nối trong mạng, bao gồm cả máy in hóa đơn và văn phòng.

Dưới đây là ví dụ về thông báo đòi tiền chuộc của hoạt động ransomware này:

```
                    LockBit Black Ransomware

                Your data are stolen and encrypted
            The data will be published on TOR website
hxxp://LockBitapt2yfbt7lchxejug47kmqvqqxvvjpqkmevv4l3azl3gy6pyd[.]onion
        and hxxp://LockBitapt[.]uz if you do not pay the ransom

  You can contact us and decrypt one file for free on these TOR sites
hxxp://LockBitsupa7e3b4pkn4mgkgojrl5iqgx24clbzc4xm7i6jeetsia3qd[.]onion
hxxp://LockBitsupn2h6be2cnqpvncyhj4rgmnwn44633hnzzmtxdvjoqlp7yd[.]onion
                        hxxp://LockBitsupp[.]uz

                        Decryption ID: [ID]
```

Ngoài việc thông báo đòi tiền chuộc được triển khai trên các thiết bị, Tina Turner còn gửi các thông tin đòi tiền chuộc qua email. Trong một số cuộc tấn công, các kẻ tấn công cũng dùng WhatsApp để trao đổi đàm phán các thông tin tiền chuộc với nạn nhân.

Dưới đây là các địa chỉ email được xác định trong một số cuộc tấn công (tên của cụm hoạt động cũng được đặt dựa trên chúng):

- tinanews[@]ro.ru
- tinanews[@]privatemail.co

Nạn nhân của hoạt động này trải rộng trên nhiều lĩnh vực khác nhau với trọng tâm là các doanh nghiệp vừa và nhỏ (SMB). Các cuộc tấn công đã được phát hiện trong lĩnh vực chăm sóc sức khỏe, nông nghiệp và thực phẩm. Tina Turner thường nhắm mục tiêu vào các lĩnh vực mà theo dự đoán sẽ mang lại lợi nhuận từ nhu cầu giải mã dữ liệu. g.

Trong các chiến dịch ransomware này, tác nhân đe dọa đã sử dụng rất nhiều các công cụ và kỹ thuật khác nhau để xâm nhập và leo thang vào hệ thống nhằm đạt được mục đích.

Phần III: Phòng chống, giảm thiểu rủi ro từ tấn công Ransomware

Cuộc tấn công Ransomware hiện nay thường được bắt đầu từ một điểm yếu bảo mật của cơ quan, tổ chức, kẻ tấn công xâm nhập hệ thống, duy trì sự hiện diện, mở rộng phạm vi xâm nhập, và kiểm soát hạ tầng công nghệ thông tin của tổ chức, làm tê liệt hệ thống, nhằm bắt buộc các tổ chức nạn nhân thực hiện hành vi tống tiền mà kẻ tấn công hướng tới.

Cục An toàn thông tin đã xây dựng Cẩm nang về một số biện pháp phòng chống, giảm thiểu rủi ro từ tấn công Ransomware cho các cơ quan, tổ chức, doanh nghiệp, hướng đến mục tiêu bảo đảm an toàn không gian mạng quốc gia, gồm các nội dung chính:

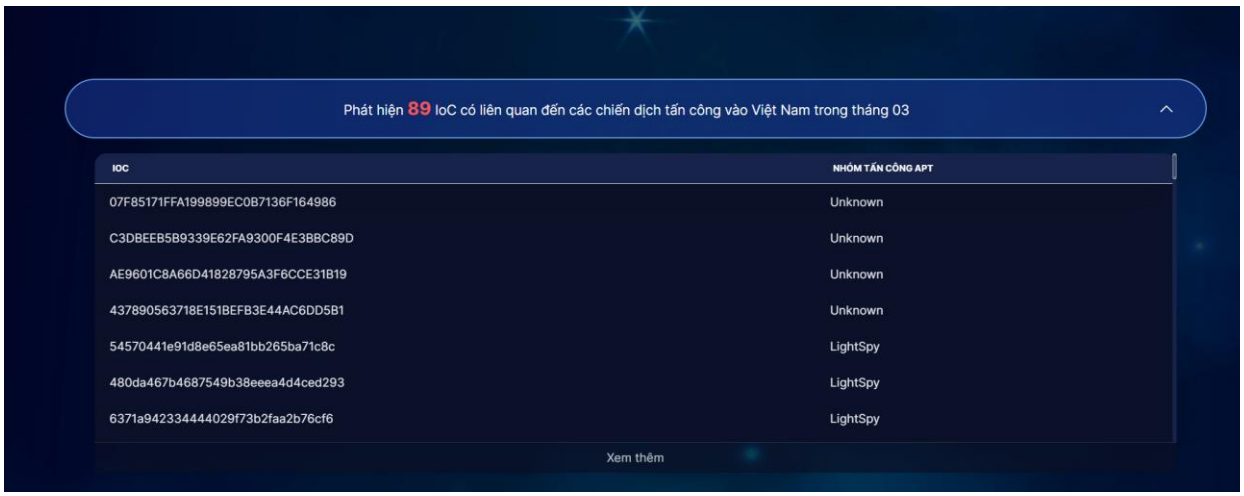
- Xây dựng kế hoạch **sao lưu**, **phục hồi dữ liệu** đối với hệ thống, thông tin quan trọng.
- Triển khai các biện pháp **xác thực mạnh** cho các tài khoản truy cập hệ thống.
- Chủ động tìm kiếm dấu hiệu tấn công, rà quét mã độc, yêu cầu đơn vị chuyên trách xử lý các mã độc.
- Giám sát liên tục để phát hiện sớm các hành vi xâm nhập, đặc biệt giám sát các truy cập đến **vCenter, ESXI, Domain Control-**
- **Rà quét, cập nhật** bản vá lỗ hổng an toàn thông tin trên các thiết bị, phần mềm, ứng dụng.
- **Xây dựng kế hoạch** ứng phó sự cố để kịp thời phản ứng với sự cố Ransomware.
- Áp dụng các **nguyên tắc đặc quyền** tối thiểu cho các hệ thống.
- **Hạn chế** việc sử dụng **dịch vụ** điều khiển máy tính **từ xa**.
- Thực hiện **phân vùng** mạng chặt chẽ.

Chi tiết cẩm nang tham khảo tại:

https://khonggianmang.vn/uploads/CAM_NANG_RANSOMWARE_fdd46cec50.pdf

Phần IV: Danh sách các chỉ báo tấn công mạng liên quan đến LockBit 3.0 đã ghi nhận

Dưới đây là một số chỉ báo tấn công mạng liên quan đến Lockbit 3.0 đã được ghi nhận. Các thông tin chỉ báo IOC sẽ liên tục được cập nhật tại: https://alert.khonggianmang.vn/



Bảng danh sách IoC

IOC	Nhóm
eba009694cdfd31348be84d3bd86765a	Lockbit 3.0
91d7df238b2b0b8ad8d1c14cbc1d98d3	Lockbit 3.0
c9cf839f1e2556dcc936d30f7692647c	Lockbit 3.0
15a9ab4601ec7e68fa8d2d2e3859fadd	Lockbit 3.0
40e92d4f37abd64e6c75ece969a6c4b3	Lockbit 3.0
4107b5b413ab08dc292cb3aabe5b2a74	Lockbit 3.0
a8f9ffcf21041ed00b900f15ba26feab	Lockbit 3.0
cf9700013fe1009f24dff061835c3ce4	Lockbit 3.0
64ee6099dade74323f3481fcdd9caf2e	Lockbit 3.0
39e92066b2eb722fbd63918f7d5065d1	Lockbit 3.0
9d38831f08f6e7f99186e5145fc802bf	Lockbit 3.0
e200af4c00627a1460fb1dd77ef36609	Lockbit 3.0
4b7932336aba193b42d8752d8cd92fdf	Lockbit 3.0
9b94fb645c8fbe4581963ef7ac96af0f	Lockbit 3.0
cc9f1499131552e399d9bf413bbec9d3	Lockbit 3.0
54022eb0e10cf69e2a4a86660da0d88e	Lockbit 3.0
abfd3d8be76dbac47500a36b17ed454f	Lockbit 3.0

Phần IV: Danh sách các chỉ báo tấn công mạng liên quan đến LockBit 3.0 đã ghi nhận

Bảng danh sách IoC

IOC	Nhóm
d8700a0f6d578c111e383c12d36a3ad0	Lockbit 3.0
714eaf666a2a195d57bd7b20455d409e	Lockbit 3.0
90b7d07904810bb2b6e4cfbcdaf34c45	Lockbit 3.0
c9637dbb7b567da3766c4969de7b0fff	Lockbit 3.0
84fcdeae85233ce2622f77de22cc1e8a	Lockbit 3.0
627c542bb564ab9513e46893f40c4617	Lockbit 3.0
eb5c016a4709ad47b3b96872badd664c	Lockbit 3.0
6a801424860b7e86639254592bbc84b1	Lockbit 3.0
87ef8b973db67b8b7cdef2dc4ac77016	Lockbit 3.0
ebff7291dcdda73f5629e87f7de659b5	Lockbit 3.0
9523d310e59ebc4538af38d0e31caaf1	Lockbit 3.0
c64e62833ca51ed6fd0a05436952b6a3	Lockbit 3.0
b8e47f43cea7df7605a9aa94f3318ae7	Lockbit 3.0
672546bd748a57a0fe39a00e8d691618	Lockbit 3.0
087793a9068821217a66a1a2e601d5ea	Lockbit 3.0
3df94bcdf20a47e67ac894788480f931	Lockbit 3.0
b53c3d548c8c3299a0ba7c0dae0c630e	Lockbit 3.0
3ebc3faa8ebd338d2e64c0034d3e9866	Lockbit 3.0
7acc6093d1bc18866cdd3feccb6da26a	Lockbit 3.0
01259980eb29aa097484d9896d376287	Lockbit 3.0
797cc745ff64c470314e7eb99ce98fc8	Lockbit 3.0
c5752a3fa1ae8542c70f7d3ca5cb56af	Lockbit 3.0
yejosowon[.]co	Lockbit 3.0
104[.]238[.]35[.]29	Lockbit 3.0
37[.]1[.]212[.]18	Lockbit 3.0
119[.]91[.]138[.]133	Lockbit 3.0