Incident Response Techniques for Ransomware Attacks

Understand modern ransomware attacks and build an incident response strategy to work through them

Oleg Skulkin

Incident Response Techniques for Ransomware Attacks

Understand modern ransomware attacks and build an incident response strategy to work through them

Oleg Skulkin

Packt

BIRMINGHAM—MUMBAI

Incident Response Techniques for Ransomware Attacks

Copyright © 2022 Packt Publishing

All rights reserved. No part of this book may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, without the prior written permission of the publisher, except in the case of brief quotations embedded in critical articles or reviews.

Every effort has been made in the preparation of this book to ensure the accuracy of the information presented. However, the information contained in this book is sold without warranty, either express or implied. Neither the author, nor Packt Publishing or its dealers and distributors, will be held liable for any damages caused or alleged to have been caused directly or indirectly by this book.

Packt Publishing has endeavored to provide trademark information about all of the companies and products mentioned in this book by the appropriate use of capitals. However, Packt Publishing cannot guarantee the accuracy of this information.

Group Product Manager: Vijin Boricha

Publishing Product Manager: Shrilekha Inani

Senior Editor: Sangeeta Purkayastha

Content Development Editor: Nihar Kapadia

Technical Editor: Shruthi Shetty

Copy Editor: Safis Editing

Project Coordinator: Shagun Saini

Proofreader: Safis Editing

Indexer: Pratik Shirodkar

Production Designer: Alishon Mendonca

Marketing Coordinator: Hemangi Lotlikar

First published: March 2022

Production reference: 1090322

Published by Packt Publishing Ltd.
Livery Place
35 Livery Street
Birmingham
B3 2PB, UK.

ISBN 978-1-80324-044-2

www.packt.com

Contributors

About the author

Oleg Skulkin is the head of the Digital Forensics and Incident Response Team at Group-IB. Oleg has worked in the fields of digital forensics, incident response, and cyber threat intelligence and research for over a decade, fueling his passion for uncovering new techniques used by hidden adversaries. Oleg has authored and coauthored multiple blog posts, papers, and books on related topics and holds GCFA and GCTI certifications. You can contact him on Twitter at `oskulkin`.

I would like to thank my team at Group-IB, as well as other colleagues from various cyber security companies, who always inspire me with their outstanding research. Also, I would like to thank the Packt team for this opportunity and their help, as well as Ricoh Danielson, who provided very valuable feedback as the technical reviewer.

6
Collecting Ransomware-Related Cyber Threat Intelligence

As you've learned from the previous chapter, **ransomware affiliates** may use a wide variety of **tactics, techniques, and procedures** (**TTPs**), so knowing what exactly they are using in the attack you are responding to seems quite a good idea. Some of these tactics and techniques might be for short games, while others may be for long-term positions—it really depends upon the end goal of the threat actor.

Usually, the first thing you learn starting an **incident response** (**IR**) engagement is the ransomware strain used by threat actors. As many ransomware strains are distributed under a **ransomware-as-a-service** (**RaaS**) model, various affiliates may have various approaches to the attack life cycle, so their TTPs may vary as well.

Taking this fact into consideration, it's a very good idea to have proper **cyber threat intelligence** (**CTI**) to aid your engagement. Of course, commercial CTI platforms are of great help, but even these sources may not have all information you may need, so the ability to collect proper intelligence for your current or future IR engagements is a key skill.

In this chapter, we'll look at some sources of ransomware-related CTI, including the following:

- Threat research reports
- Community
- Threat actors

Threat research reports

Most cyber security companies produce various threat research reports, including those related to ransomware attacks, so such sources can be easily used for CTI collection. Threat research reports are a very important part of threat assessment. These reports help technical and non-technical people to assess their current landscape and measure it against the threat landscape.

Of course, no report contains all the details, so the best approach is to use research produced by various cyber security vendors focused on the same threat. At the same time, some reports provide **indicators of compromise** (**IoCs**) and other critical data that can be shared with the general public. Some of these reports can help others be prepared for these threat actors and their attacks.

In this section, we'll look at various reports on **Egregor ransomware** so that we can collect as much intelligence on its affiliates' TTPs as possible.

Let's start with the report by *Group-IB* I co-authored, which is titled *Egregor ransomware: The legacy of Maze lives on*. The report is available here: `https://explore.group-ib.com/ransomware-reports/egregor_wp`.

Every ransomware attack starts from initial access to the target network. According to the report we are analyzing, Egregor affiliates used **Qakbot**, which was delivered to victims via spear-phishing emails. Spear phishing is one of the most common yet highly effective means to gain access to a network. These threat actors know that they can target regular users because they know they might not have the technical skills to understand an attack.

So, what is Qakbot? Originally, it's a banking trojan that was first observed in the wild in 2007. Currently, it's used mostly for downloading additional payloads—for example, **Cobalt Strike Beacon**, and performing mass spamming activities using compromised hosts in order to infect additional targets. This trojan is notoriously used for gaining initial access to target networks by many ransomware affiliates, including **ProLock**, **Egregor**, **REvil**, **Conti**, and others.

The *Group-IB* report also contains information on Qakbot's persistence mechanisms, which include putting the payload or a **link** (**LNK**) file to the `startup` folder, writing the path to the payload in the *Run* key, or creating a scheduled task.

Post-exploitation activities include the use of Cobalt Strike. It's a commercial full-featured post-exploitation framework that originally was a tool for emulation of advanced attacks but soon became one of the most common tools in real threat actors' arsenal, enabling them to use many techniques described in *MITRE ATT&CK*.

According to the report, the threat actors also used **ADFind** to collect information about the compromised **Active Directory** (**AD**) environment. As you've learned from the previous chapter, this tool is also quite common for human-operated ransomware attacks.

To enable lateral movement, Egregor affiliates used scripting to make proper registry and firewall changes so that they could use **Remote Desktop Protocol** (**RDP**). The scripts are distributed via **PsExec**, a legitimate tool from **Sysinternals Suite** that allows you to execute commands on remote hosts. Legitimate tools and various scripts are the main means that threat actors use to stay undetected.

Another common technique observed to be used by Egregor affiliates is **process injection**, which is enabled by Cobalt Strike Beacon. Cobalt Strike Beacon can be a very powerful tool when trying to start lateral movement across an environment. Such techniques allow threat actors to be able to hide commands they use so that they can stay unnoticed.

To exfiltrate sensitive data from the network, Egregor affiliates used **Rclone**, a command-line tool for managing files on cloud storage. What's more, they use masquerading techniques, renaming the Rclone executable to `svchost.exe`.

To disable antivirus protection, the threat actors leveraged Group Policy, as well as `scepinstall.exe`, to uninstall **System Center Endpoint Protection** (**SCEP**). Such attacks are another example of how threat actors abuse legitimate features of modern environments.

To deploy ransomware, Egregor affiliates used a variety of techniques enabled by scripting, including the following:

- Abusing **Background Intelligent Transfer Service** (**BITS**) to download the ransomware payload from the attacker-controlled server and run it via `rundll32`
- Mounting the `C:\` drive of a remote host as a network share, copying the payload to `C:\Windows`, and running it via `rundll32`
- Copying and executing the ransomware payload via a PowerShell session on a remote host

As you can see, we can collect a lot of intelligence from just one single report, but of course, we can enrich it with more data.

Let's look at another report, this time from *Cybereason*, titled *Cybereason vs. Egregor Ransomware*. The report is available here: `https://www.cybereason.com/blog/cybereason-vs-egregor-ransomware`.

Now, we need to analyze it, extract data that we still don't have, and transform it into actionable CTI.

First of all, we can see that, according to the *Cybereason* report, Egregor affiliates obtain initial access to the target networks not only via Qakbot infections but also via **Ursnif** and **IcedID**. Just as with Qakbot, both malware families used to be banking trojans but are now usually used for downloading additional payloads. As we can see, many threat actors develop new capabilities, so their attacks can be more and more profitable.

Also, according to the report, Egregor affiliates use **SharpHound** (the data collector for BloodHound, which is commonly used by pen testers and threat actors to find relationships within an AD environment) to gather information about users, groups, computers, and so on.

Good—we've collected even more CTI, but let's go forward and look at one more report. This time, it's a report on Egregor ransomware by *Morphisec* titled *An analysis of the Egregor ransomware*. The report is available here: `https://www.morphisec.com/hubfs/eBooks_and_Whitepapers/EGREGOR%20REPORT%20WEB%20FINAL.pdf`.

According to this report, Egregor affiliates obtained initial access via exploitation of a non-pathed **virtual private network** (**VPN**), so there are no trojans this time.

The threat actors used legitimate remote access software, such as **AnyDesk** and **SupRemo**, to maintain access to the compromised network. In 2021, AnyDesk was one of the most common tools leveraged by threat actors for redundant access.

To disable unwanted processes (for example, those belonging to antivirus software), the attackers used **PowerTool**—a free anti-rootkit utility.

To collect information about the compromised network, the threat actors leveraged a popular free tool—**SoftPerfect Network Scanner**.

To enable credential dumping, Egregor affiliates used **Mimikatz**, another popular tool used by pen testers and threat actors to extract passwords from memory, as well as other authentication material—hashes, **personal identification numbers** (**PINs**), and Kerberos tickets.

For data exfiltration, the threat actors used various cloud services, such as **WeTransfer** and **SendSpace**, as well as **MEGA Desktop App**.

In this case, Egregor affiliates also leveraged PsExec to execute scripts on remote hosts that ran the ransomware payload.

Finally, to cover some traces, the threat actors used `SDelete`—a command-line utility for secure file deletion.

OK—let's summarize our findings based on the analysis of all three reports, as follows:

- Egregor affiliates obtain initial access either via infecting the target hosts with various trojans using phishing emails or by exploiting non-patched VPNs.
- Egregor affiliates use various persistence mechanisms, including a startup folder, the *Run* key, and scheduled tasks.
- To collect information about compromised networks and AD, Egregor affiliates use ADFind, SharpHound, and SoftPerfect Network Scanner.
- To enable various post-exploitation activities, Egregor affiliates use Cobalt Strike.
- Egregor affiliates use RDP for lateral movement.
- Egregor affiliates use PsExec to execute commands and scripts, including those for ransomware deployment.

- Egregor affiliates use Group Policy and PowerTool to disable antivirus software, as well as `scepinstall.exe` to uninstall SCEP.
- Egregor affiliates use AnyDesk and SupRemo to maintain access to the compromised network.
- Egregor affiliates use Rclone and MEGA Desktop App, as well as various cloud services, for data exfiltration.
- To deploy ransomware, Egregor affiliates use BITS, PowerShell remoting, network shares, and `rundll32`.

As you can see, analyzing reports from various cyber security companies may provide us with great insights into ransomware affiliates' operations for us to use this CTI to make our IR engagements faster and more efficient.

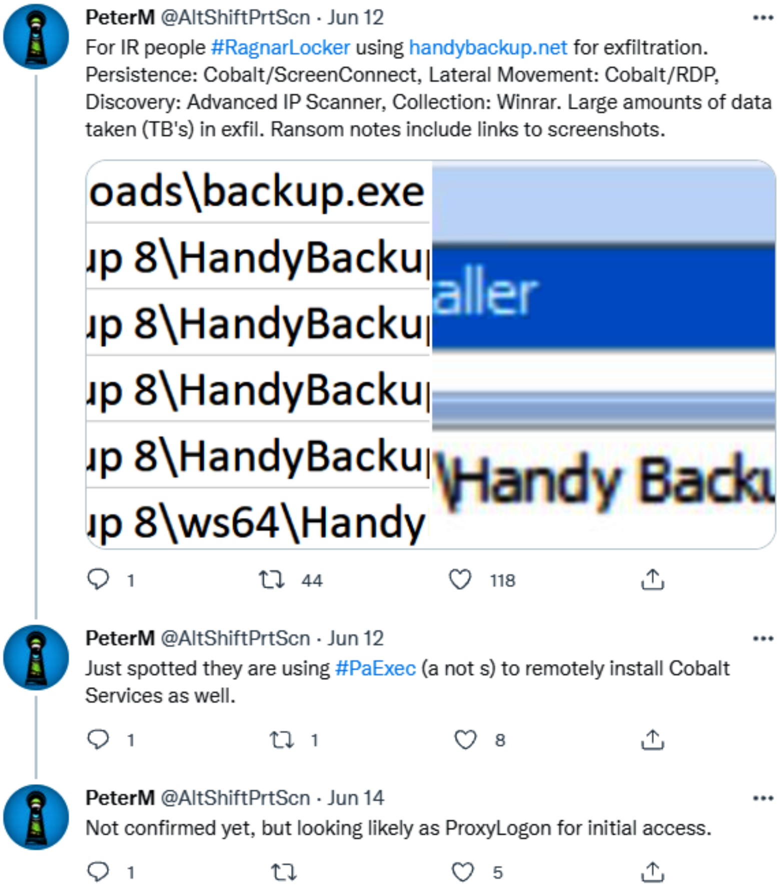
In the next section, we'll look at how we can collect CTI from the cyber security community.

Community

There are thousands of incident responders worldwide, and of course, some of them like to share their findings from IR engagements. We already looked at some threat research reports, but it usually takes quite a lot of time to create one. Therefore, responders and researchers often use other media to share their findings in a short form. A very popular media platform for such sharing is *Twitter*.

If you are dealing with a human-operated ransomware attack and you already identified the strain, you may find quite a lot of information on the threat actors, including TTPs. Understanding the threat actor is critical. Usually, certain ransomware affiliates use specific tools and processes during certain stages of the attack life cycle.

Let's start with **RagnarLocker ransomware** and have a look at the following tweet from Peter Mackenzie, Director of Incident Response at *Sophos* (`https://twitter.com/AltShiftPrtScn/status/1403707430765273095`):



PeterM @AltShiftPrtScn · Jun 12

For IR people #RagnarLocker using handybackup.net for exfiltration. Persistence: Cobalt/ScreenConnect, Lateral Movement: Cobalt/RDP, Discovery: Advanced IP Scanner, Collection: Winrar. Large amounts of data taken (TB's) in exfil. Ransom notes include links to screenshots.

1 44 118

PeterM @AltShiftPrtScn · Jun 12

Just spotted they are using #PaExec (a not s) to remotely install Cobalt Services as well.

1 1 8

PeterM @AltShiftPrtScn · Jun 14

Not confirmed yet, but looking likely as ProxyLogon for initial access.

1 5

Figure 6.1 – A tweet on RagnarLocker

So, what can we learn from this tweet? First of all, we can see that RagnarLocker affiliates potentially use **ProxyLogon** (**Common Vulnerabilities and Exposures** (**CVE**) - *2021-26855*) for obtaining initial access to their targets. ProxyLogon is a vulnerability in Microsoft Exchange Server that allows an attacker to bypass authentication and impersonate the administrator.

To collect information about internal networks, RagnarLocker affiliates use **Advanced IP Scanner**, a free network scanner from *Famatech Corp* that is quite popular among various RaaS programs' affiliates.

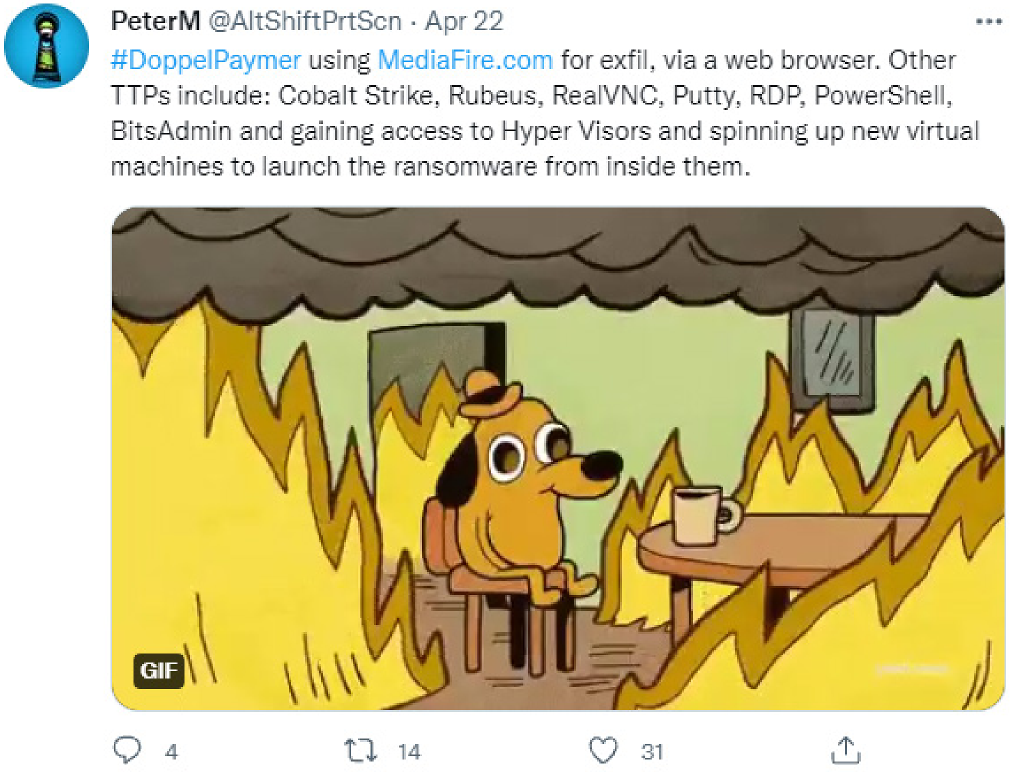
Just as with many other threat actors, RagnarLocker affiliates use Cobalt Strike for various post-exploitation activities, including lateral movement (alongside RDP). To distribute beacons on remote hosts, the threat actors use **PaExec**, an open source alternative to PsExec from Sysinternals.

To have redundant access to a compromised network, RagnarLocker affiliates use **ScreenConnect**, legitimate remote-control software. Despite the fact it is legitimate, it can be leveraged by threat actors to obtain access to a compromised network.

Collected sensitive data is archived with help of **WinRAR** and exfiltrated with the help of **Handy Backup**, a commercial backup solution installed on the target hosts by threat actors. Zipping and password-protecting are common techniques used by threat actors during the exfiltration phase. Still, there are a lot of various forensic artifacts sources that can be used to detect it.

As you can see, we can collect a lot of valuable information from just a few tweets.

Let's move forward and look at another tweet by the same author, which you can see here:



PeterM @AltShiftPrtScn · Apr 22

#DoppelPaymer using MediaFire.com for exfil, via a web browser. Other TTPs include: Cobalt Strike, Rubeus, RealVNC, Putty, RDP, PowerShell, BitsAdmin and gaining access to Hyper Visors and spinning up new virtual machines to launch the ransomware from inside them.

Figure 6.2 – A tweet on DoppelPaymer

Just as with RagnarLocker affiliates, **DoppelPaymer** affiliates actively use Cobalt Strike for post-exploitation.

Also, we can see that threat actors use **Rubeus**, a quite popular toolset for interacting with and abusing Kerberos.

Here's another example of a legitimate remote access tool used by threat actors for redundant access—**TightVNC**.

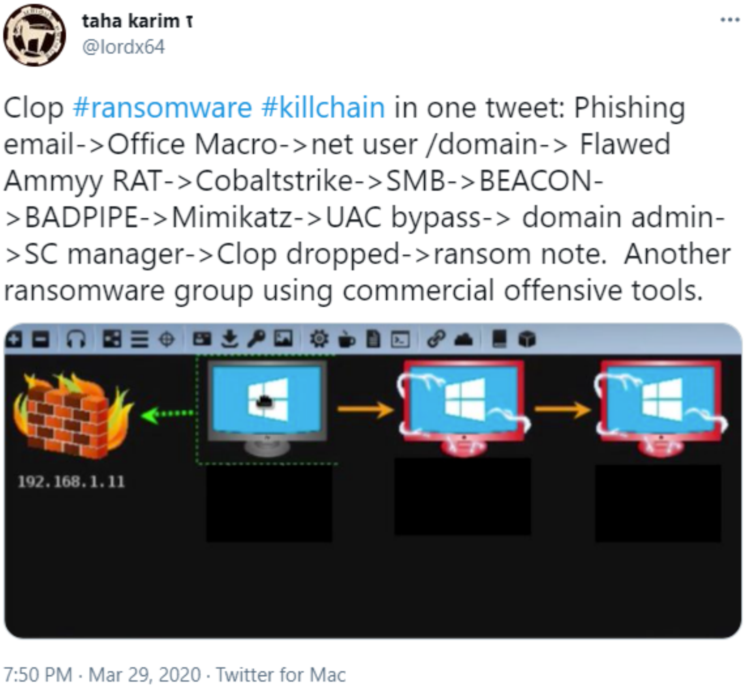
Again, we can see that DoppelPaymer affiliates use RDP for lateral movement—a very common technique used by threat actors both for initial access and accessing remote hosts in the target network.

Another interesting technique mentioned is creating a **virtual machine** (**VM**) to run the ransomware payload inside it. Originally, this technique was introduced by Maze and RagnarLocker affiliates, but it's currently used by other groups, including DoppelPaymer, as well.

Just as with many other threat actors, DoppelPaymer affiliates have a **Dedicated Leak Site** (**DLS**), so they exfiltrate data. From the source we are analyzing, we can see that they use the **MediaFire** service to store data.

One more time, we can see that we can collect a lot of valuable data on this or that threat actor involved in ransomware attacks, from just a single tweet.

Let's look at one more example, this time a tweet from Taha Karim, Director of Threat Intelligence at *Confiant*, which you can see here:



taha karim
@lordx64

Clop #ransomware #killchain in one tweet: Phishing email->Office Macro->net user /domain-> Flawed Ammyy RAT->Cobaltstrike->SMB->BEACON->BADPIPE->Mimikatz->UAC bypass-> domain admin->SC manager->Clop dropped->ransom note. Another ransomware group using commercial offensive tools.

7:50 PM · Mar 29, 2020 · Twitter for Mac

Figure 6.3 – A tweet on Clop

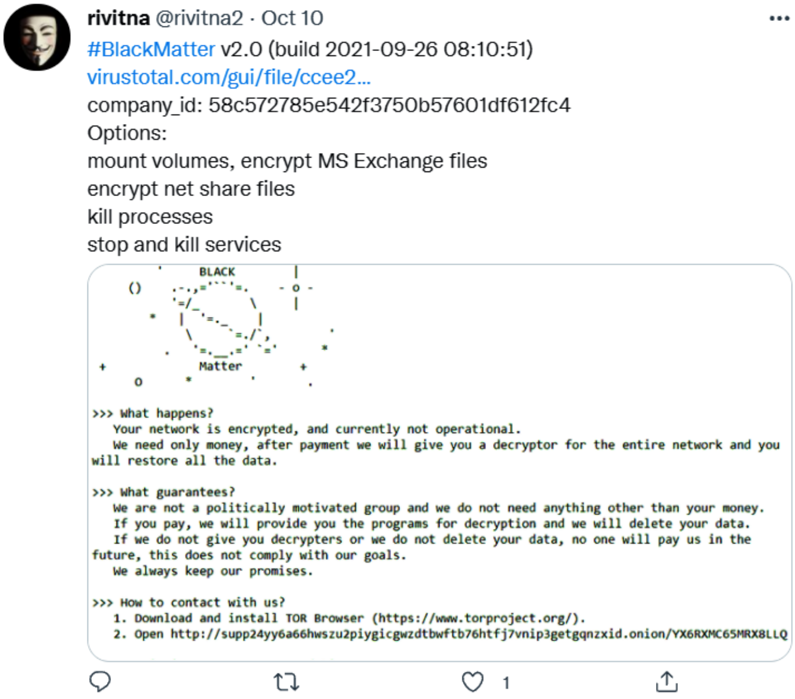
It's interesting that this tweet emerged long before any information on Clop affiliates' TTPs was published publicly.

As we can see from the tweet, Clop affiliates used phishing campaigns to infect their victims with **FlawedAmmyy RAT**. FlawedAmmyy is a common **remote access trojan** (**RAT**), usually attributed to TA505. The RAT is based on Ammyy Admin's leaked source code and enables threat actors to manipulate the compromised host in a hidden manner.

We have already learned that ransomware affiliates are in love with Cobalt Strike, and Clop ransomware affiliates are no exception. As you can see, it enables them to bypass **User Account Control** (**UAC**) and use common credential dumping tools such as Mimikatz. Despite the fact it's very noisy, we still see it leveraged by ransomware affiliates very often.

Finally, we can learn that Clop affiliates abuse **Service Control Manager** (**SCM**) to deploy ransomware enterprise-wide.

Of course, it's not always possible to collect a lot of information about the TTPs used by threat actors during the attack life cycle. At the same time, you may need to get some information about the ransomware itself. Here's a tweet by Andrew Zhdanov, who is actively tracking **BlackMatter ransomware** samples:



rivitna @rivitna2 · Oct 10

#BlackMatter v2.0 (build 2021-09-26 08:10:51)
virustotal.com/gui/file/ccee2...
company_id: 58c572785e542f3750b57601df612fc4
Options:
mount volumes, encrypt MS Exchange files
encrypt net share files
kill processes
stop and kill services

```
>>> What happens?
   Your network is encrypted, and currently not operational.
   We need only money, after payment we will give you a decryptor for the entire network and you
will restore all the data.

>>> What guarantees?
   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 we will delete your data.
   If we do not give you decrypters or we do not delete your data, no one will pay us in the
future, this does not comply with our goals.
   We always keep our promises.

>>> How to contact with us?
   1. Download and install TOR Browser (https://www.torproject.org/).
   2. Open http://supp24yy6a66hwszu2piygicgwzdtbwftb76htfj7vnip3getgqnzxid.onion/YX6RXMC65MRX8LLQ
```

Figure 6.4 – A tweet on BlackMatter

As you can see, there's not a lot of information on TTPs, but the tweet contains a link to the analyzed sample, as well as information on some of its functionality.

Twitter isn't the only media platform for such intelligence collection—another good example is *LinkedIn*. Also, you can always ask your fellow incident responders and CTI analysts to share some data—just don't be afraid of the global community.

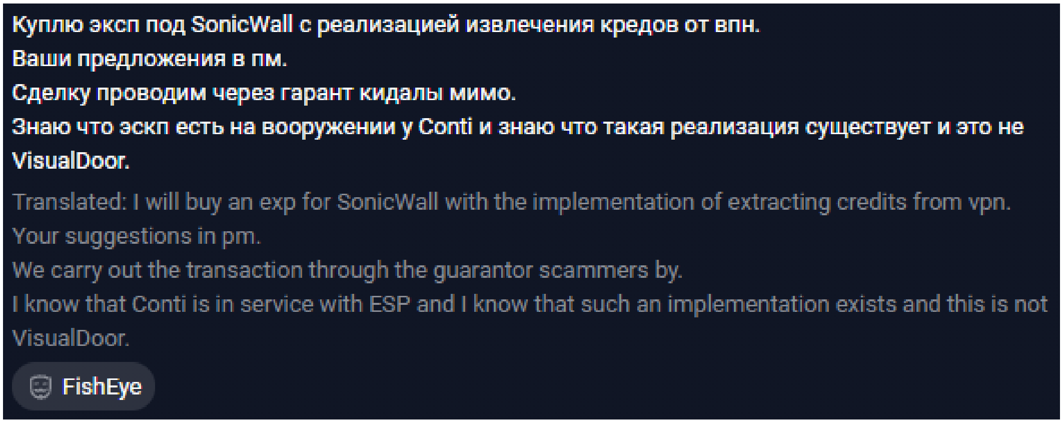
Now let's look at an even more interesting source of actionable CTI—the threat actors themselves.

Threat actors

As you will have understood already, this book is devoted to human-operated ransomware attacks. So, the threat actors we are dealing with are humans, and humans tend to communicate and share. One of the most common media used for such sharing is underground forums.

In this section, we'll look at some forum posts, collected by the **Group-IB Threat Intelligence and Attribution** platform.

The first post we'll look at is created by a threat actor with the nickname *FishEye*, who is known to be affiliated with REvil, LockBit, and some other ransomware strains. You can see it here:



Куплю эксп под SonicWall с реализацией извлечения кредов от впн.
Ваши предложения в пм.
Сделку проводим через гарант кидалы мимо.
Знаю что эскп есть на вооружении у Conti и знаю что такая реализация существует и это не VisualDoor.

Translated: I will buy an exp for SonicWall with the implementation of extracting credits from vpn.
Your suggestions in pm.
We carry out the transaction through the guarantor scammers by.
I know that Conti is in service with ESP and I know that such an implementation exists and this is not VisualDoor.

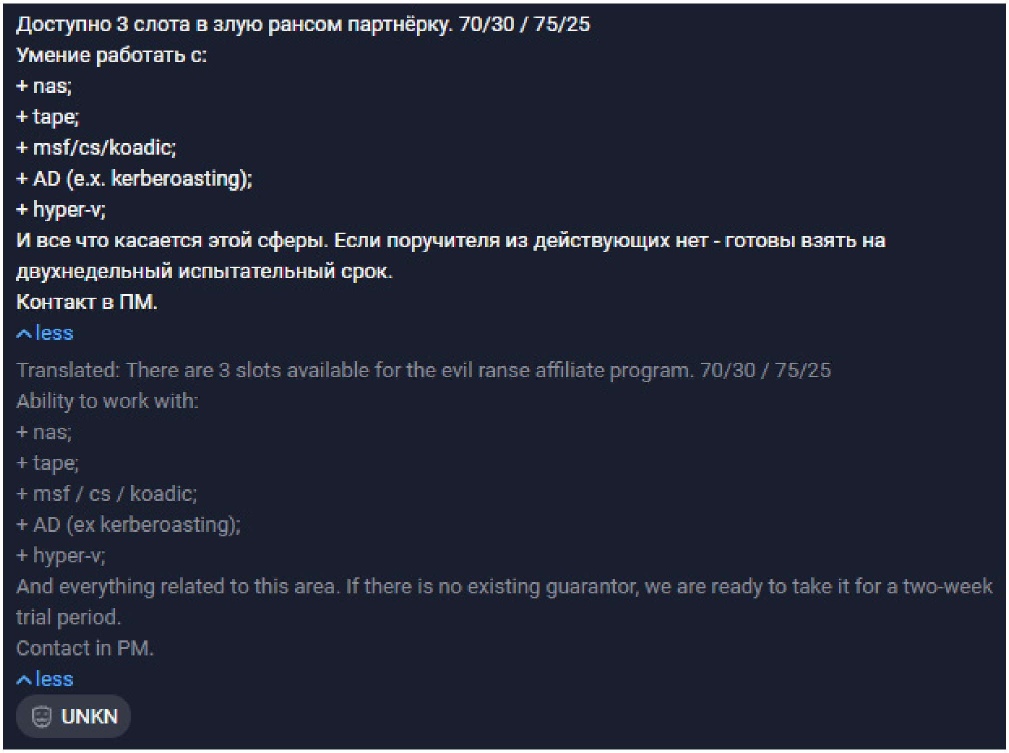
FishEye

Figure 6.5 – A post by FishEye

In this post, the threat actor shows their interest in obtaining a working exploit for a vulnerability in the **SonicWall VPN**. The threat actor points out the fact that Conti ransomware affiliates already have it and use it in their campaigns.

Most likely, the threat actor is writing about a vulnerability in SonicWall **Secure Mobile Access** (**SMA**) 100-series products (*CVE-2021-20016*). This vulnerability can be exploited remotely and enables attackers to access credentials so that they can access the internal network using valid accounts to perform post-exploitation actions.

The next post we'll look at is one by a notorious REvil spokesperson under the moniker *UNKN*. Here it is:



Доступно 3 слота в злую рансом партнёрку. 70/30 / 75/25
Умение работать с:
+ nas;
+ tape;
+ msf/cs/koadic;
+ AD (e.x. kerberoasting);
+ hyper-v;
И все что касается этой сферы. Если поручителя из действующих нет - готовы взять на двухнедельный испытательный срок.
Контакт в ПМ.
^ less

Translated: There are 3 slots available for the evil ranse affiliate program. 70/30 / 75/25
Ability to work with:
+ nas;
+ tape;
+ msf / cs / koadic;
+ AD (ex kerberoasting);
+ hyper-v;
And everything related to this area. If there is no existing guarantor, we are ready to take it for a two-week trial period.
Contact in PM.
^ less

Figure 6.6 – A post by UNKN

This post advertises the REvil RaaS program and depicts the requirements for affiliates. First of all, we can see that potential affiliates must be aware of common data storage types, which are commonly used for storing backups. These include **network-attached storage** (**NAS**) and **tape-based data storage**.

Next, the threat actor notes that potential affiliates should be ready to use various post-exploitation frameworks. Here are some examples of these:

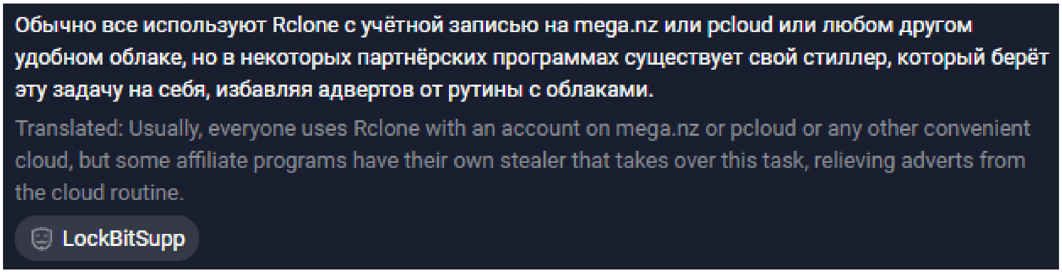
- Metasploit Framework
- Cobalt Strike
- Koadic

Also, affiliates should be able to perform attacks against AD environments, including **kerberoasting attacks**, which allow threat actors to extract service account credential hashes and use them to crack passwords offline.

Finally, as many modern corporate environments use virtualization, the ability to understand and attack technologies such as **Hyper-V** is a must for affiliates.

As you can see, in some cases, threat actors share quite a lot of information on their affiliates' potential TTPs.

Another thing threat actors commonly do is comment on various problems presented by other forum members. For example, here is an opinion on data exfiltration techniques by a **LockBit ransomware** representative under the moniker *LockBitSupp*:



Обычно все используют Rclone с учётной записью на mega.nz или pcloud или любом другом удобном облаке, но в некоторых партнёрских программах существует свой стиллер, который берёт эту задачу на себя, избавляя адвертов от рутины с облаками.

Translated: Usually, everyone uses Rclone with an account on mega.nz or pcloud or any other convenient cloud, but some affiliate programs have their own stealer that takes over this task, relieving adverts from the cloud routine.

LockBitSupp

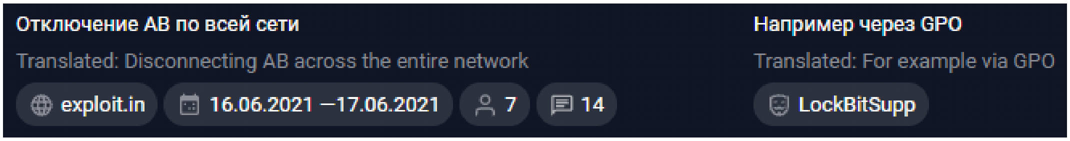
Figure 6.7 – A post by LockBitSupp

In the post, the threat actor describes a common process leveraged by ransomware affiliates to exfiltrate data from a compromised network. According to the actor, affiliates usually use Rclone and accounts from common cloud storage providers, such as **MEGA** and **pCloud**.

At the same time, the threat actor notes that some RaaS programs offer custom stealers for data exfiltration.

In fact, they are just trying to advertise **StealBit**, a custom exfiltration tool offered to LockBit ransomware affiliates.

Another post by the same threat actor is devoted to disabling antivirus software enterprise-wide, as we can see here:



Отключение АВ по всей сети

Translated: Disconnecting AB across the entire network

exploit.in 16.06.2021 —17.06.2021 7 14

Например через GPO

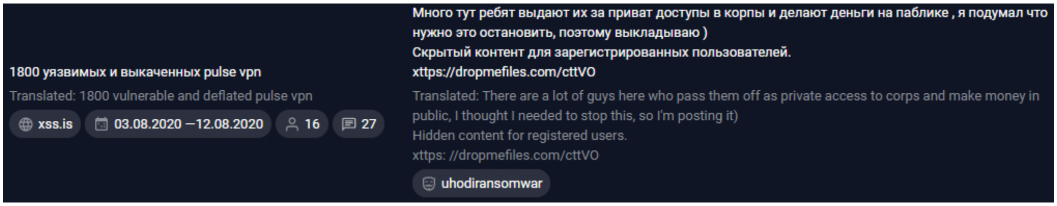
Translated: For example via GPO

LockBitSupp

Figure 6.8 – A post by LockBitSupp

Abusing **Group Policy Objects** (**GPOs**) is indeed a very common way of executing various scripts enterprise-wide and not just disabling security products. Interestingly enough, the LockBit ransomware itself has a built-in capability to abuse GPOs to distribute itself through the enterprise network.

The last post we are going to look at is a post by one of LockBit ransomware's affiliates under the moniker *uhodiransomwar*, which we can see here:



1800 уязвимых и выкаченных pulse vpn

Translated: 1800 vulnerable and deflated pulse vpn

Много тут ребят выдают их за приват доступы в корпы и делают деньги на паблике , я подумал что нужно это остановить, поэтому выкладываю)
Скрытый контент для зарегистрированных пользователей.
xttps://dropmefiles.com/cttVO

Translated: There are a lot of guys here who pass them off as private access to corps and make money in public, I thought I needed to stop this, so I'm posting it)
Hidden content for registered users.
xttps: //dropmefiles.com/cttVO

Figure 6.9 – A post by uhodiransomwar

In this thread, the threat actor shares a list of compromised Pulse Secure VPN servers, so other ransomware affiliates can use them for gaining initial access to networks. Most likely, the servers were vulnerable to *CVE-2019-11510*, which allowed the threat actor to obtain legitimate credentials via arbitrary file reading.

As you can see, there are a lot of opportunities to collect actionable CTI that could be of great help in your ransomware IR engagements.

Summary

In this chapter, we have looked at various sources of ransomware-related CTI. We've analyzed a couple of open source reports and extracted valuable pieces of data to allow us to reconstruct various parts of the attack life cycle and transform them into CTI.

We've learned how to analyze social media to extract pieces of cyber threat data shared by representatives of the cyber security community.

Finally, we've looked deep into underground forums and learned how to receive CTI directly from the adversary—ransomware affiliates.

Now, as you've already learned a lot about human-operated ransomware attacks and have a clear understanding of how such attacks actually work, you are ready to dive into the process of investigation.

In the next chapter, we'll look at the main sources of digital forensic artifacts that allow incident responders to reconstruct a human-operated ransomware attack and understand what exactly was done during its life cycle.