Conti's Hacker Manuals —— Read, Reviewed & Analyzed

Written by

Stiv Kupchik

April 05, 2022

Senior Security Researcher, based in Tel Aviv, IL

Share

Executive Summary

- Akamai Security Researchers have reviewed and analyzed the leaked Conti group's internal documentation to understand the tools and techniques used by a modern ransomware group.
- Conti is a ransomware gang with revenues projected at almost 200 million dollars and is considered one of the most successful ransomware gangs in the world.
- The analysis reveals a list of concrete techniques and procedures (TTPs) and indicators of compromise (IoC) employed by the group, as well as potential mitigation techniques that can be utilized by blue teams.
- These attack scenarios are multifaceted and detail-oriented. They have found a formula that continues to work: harvest credentials, propagate, repeat.
- The attack documentation shows a strong focus on "hands on keyboard" network propagation —— hinting at the need for strong protections against lateral movement, and its critical role in defending against ransomware.
- These TTPs are well-known, but highly effective techniques. It is a sobering reminder of the arsenal that is at the disposal of attack groups like Conti, and may hint at the tools often used by other groups. Studying these TTPs offers security teams an "inside scoop" into the attackers' modus operandi in an effort to be better prepared against them.

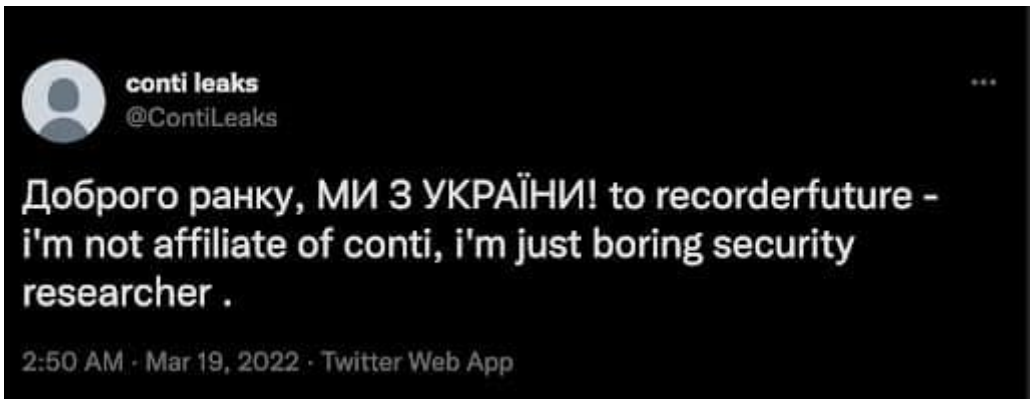
- The group's emphasis in their documentation on hacking and hands-on propagation, rather than encryption, should drive network defenders to focus on those parts of the kill chain as well, instead of focusing on the encryption phase.

Table of Contents

Introduction

Conti is a notorious ransomware group that targets high-revenue organizations. They were first detected in 2020, and appear to be based in Russia. It is believed that the group is the successor to Ryuk ransomware group. According to Chainalysis, the ransomware group was the highest grossing of all ransomware groups in 2021, with an estimated revenue of at least 180 million dollars.

On February 27, 2022, the Twitter handle @contileaks was created and began leaking internal documents and chat logs of the group, as well as the addresses of some of their internal servers and source code. It is widely accepted in the community that it was an internal member who leaked the documents after a dispute over the group's public support of the Russian government during the Russian—Ukrainian conflict, but the person behind the contileaks Twitter account claims to be an independent Ukrainian researcher.



Although leaks like this have happened in the past (usually due to personal interests of the operators), what makes this one particularly interesting is the sheer amount of information leaked. Regardless of the circumstances, these documents give the community a rare glimpse into how these attack groups operate on a grand scale, what they use, and how they think in general.

There has, understandably, been a significant amount of news coverage on these documents, particularly the chat logs, which have opened a window into the human connections inside a cybercrime group. However, not much has been written so far about the tools, techniques, and procedures of the group.

In an effort to glean this information, we decided to focus on internal documentation, which includes guidelines for operators on target selection, hacking, and using their tools. We believe that these TTPs and methodologies should also give insight into other ransomware operators, allowing us to put ourselves in the shoes of these attackers, understand their ways of operating, and prepare our defenses accordingly.

In this blog post, we discuss the attack methodology and tools used by the Conti ransomware group, as gleaned from their leaked documentation. If you'd just like to know how to defend yourself and your network, or just want a quick list of their TTPs, you can skip to our Mitigations or summary sections.

Conti's attack methodology

Like many modern cybercrime groups, Conti operates like a business. As outlined in this article from Wired, the group is capable of making profits (some operators have claimed personal gains of almost US$100 thousand), growing their operation, and adding new operators —— and even has a CEO.

As part of their business operation, Conti employs an "onboarding process" for new operators, governed by manuals detailing their methodology and modus operandi. In these manuals, we find important information on how Conti propagates inside networks, what targets they select, and what tools they use.

Interestingly, Conti is known for being a double-extortion attack group —— Conti both exfiltrates and encrypts data in order to ensure payment. The exfiltrated data is either used to blackmail a company into paying the ransom or sold to the highest bidder. In this way, even if backups are available, companies are pressured to pay in order to avoid the damage that may be caused by a leak. This method was first popularized by the Maze ransomware group, which was supposedly shut down in 2020, and from which many members were recruited into Conti.

As shown in the screenshots below, taken from Conti's site, Conti operates on a release timeline of sorts: Once they've alerted the organization of the extortion, they release more and more of the data they've exfiltrated, the longer the victim takes to pay them. The group does not appear to have a predefined ransom price guideline, with some leaked chat logs showing group members discussing the ransom price for victims.

Conti's leak website, front page

The leak features two documents that overview Conti's network attack methodology and their propagation goals. These documents are directed at the hacking operators/associates of the group. We haven't seen documentation or manuals regarding initial access practices, only design documents for various internet crawlers. We think this might indicate that this vector is somewhat automated. The operator guidelines are used after the initial breach has been made.

Both documents describe the same methodology, which can be summarized as "harvest credentials, propagate, repeat." As mentioned, an operator is assumed to have access to a machine in the network. Their goal then is to begin propagating through the network, first either by attempting to dump and

decrypt passwords or by brute force. Then, the operator is instructed to use credentials on the next machine, expanding their reach, then repeat step one. Likewise, operators are taught that encryption doesn't start until network dominance has been reached, which ensures the impact is maximized.

Conti's attack doctrine is not a novel one. The use of effective tools and persistence seems to do the trick. The process appears to be mostly "hands on keyboard" —– while some functions can be scripted or automated, operators are generally expected to do the work of stealing credentials and making cognizant decisions on spreading in the network.

Network propagation goals

First and foremost, Conti's goal is to reach the domain controller (DC). Operators are instructed to work their way to the DC via the aforementioned process of stealing credentials and expanding. Since the process seems to be largely manual, this allows Conti operators a level of discretion in choosing targets. Once the domain admin credentials are found, Conti operators will have gained access to a number of critical assets:

- Login logs for most of the network to analyze user behavior
- DNS records for most of the domain, which can be used to infer usage
- Password hashes
- Focal points for lateral movement

This focus on the DC bolsters the idea that the network propagation phase is crucial to the attack. From the DC, the attackers can extract most (if not all) the credentials they need to access the entire network. Also, as more domain configuration is usually stored there, the attackers usually gain a lot of intel about the network itself and its crown jewels.

- Interestingly, Conti discourages leaving backdoors and persistence on the DC, and instead encourages backdooring outward-facing servers since a DC is often much more heavily monitored. Although reaching the DC is pivotal to their success, it could also entirely thwart their efforts if detected.

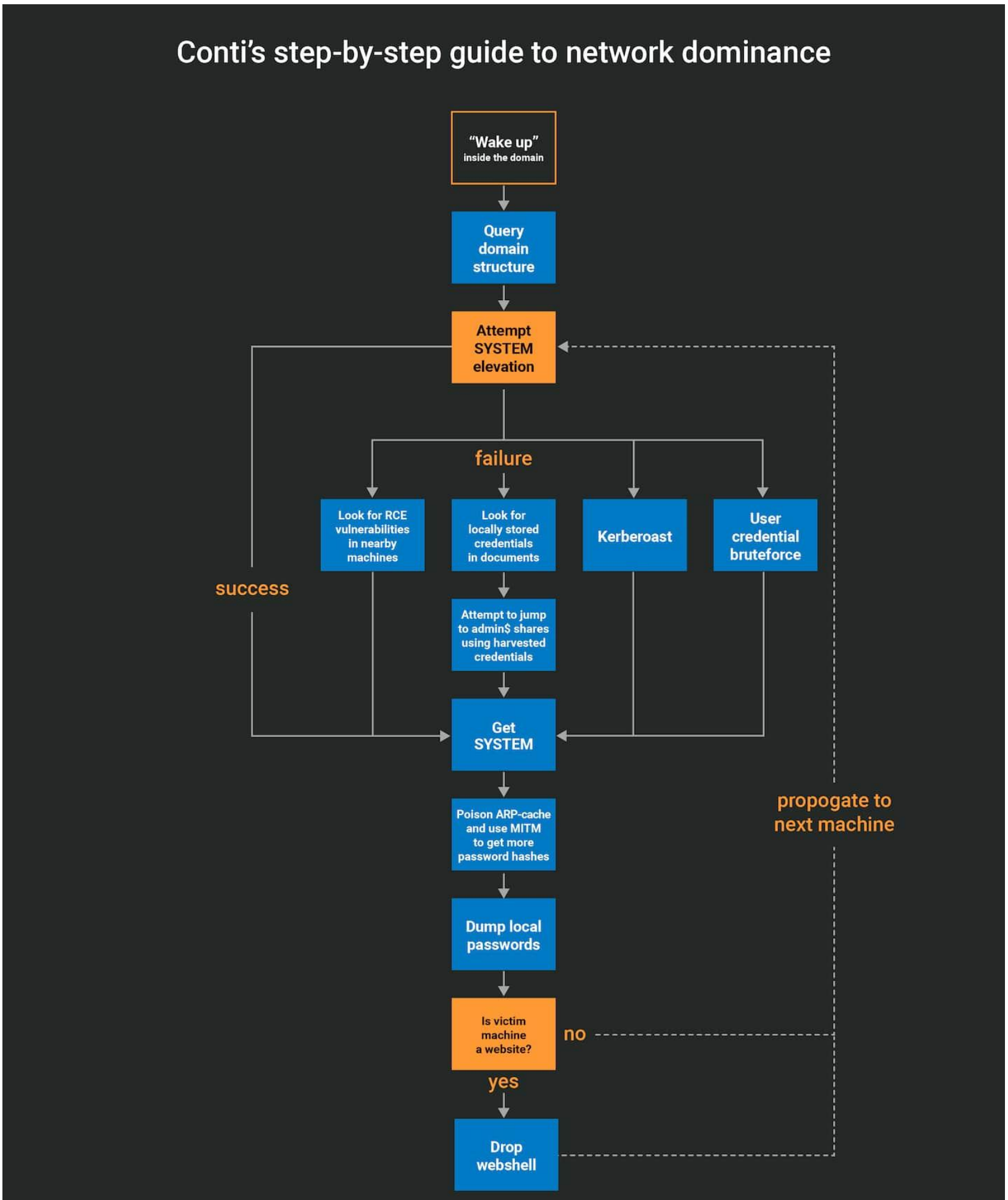
Conti defines crown jewels as network file shares and other machines that hold data that can be exfiltrated. This data includes:

- Emails, address lists, contact information
- Databases
- Source code
- Accounting information
- Design documents
- Passwords/credentials for other networks
- Digital wallets

Conti's step-by-step guide to network dominance

Conti illustrates their doctrine with a step-by-step technical guideline on gaining network dominance. The following is an almost literal translation of their method, but a bit more organized than the original text. It requires some technical understanding of the tools and processes used. However, for those concerned with defending their organization against similar attacks, or those looking to emulate a Conti attack, valuable information can be gleaned as to the type of telemetry that should appear during the lateral movement and privilege escalation phases.

It is likely that not every operator follows this to the letter, but it should shed some light on the thought process of the Conti gang. If you are more interested in how to mitigate the threat, rather than the threat itself, you can jump to our Mitigations section.



1. Query domain structure (using adfind, net view etc)

a. Sometimes passwords will appear in those tools' output immediately, under some comments

2. Try to elevate to SYSTEM rights

3. If possible:

a. Poison ARP-cache and intercept password hashes from other machines in the network

b. Dump local password hashes

4. If not:

a. Try to see if other machines in the network are accessible, specifically if their admin$ share is accessible

i. If it is, jump there to obtain SYSTEM rights

b. Look for RCE vulnerabilities in the network

c. Attempt Kerberoast to obtain more password hashes

d. For small networks, also possible to attempt brute forcing user passwords

i. There's a special emphasis on testing the lockout limits for brute force before attempting it

5. For any server with a writeable inetpub directory, drop an aspx webshell

6. Scan the network for further spread paths

Conti's toolkit

To achieve their network infiltration and propagation goals, Conti employs various tools, most of them not of Conti's own making. In fact, only the crypter, the trojan, and the injector seem to be proprietary, but for lateral movement, propagation, and exfiltration Conti seems to use a plethora of tools that should be familiar to anyone on both red and blue teams: Cobalt Strike, Mimikatz, and PSExec, to name a few.

Although some readers may expect to see 0days and proprietary tools, the leak demonstrates that a tool or technique's effectiveness is not directly correlated with how novel or unknown it is. Readers would be advised to pay close attention to the tools and techniques leaked from the Conti documentation in an effort to have more effective mitigation of these TTPs in their own defense.

- The main hacking tool in Conti's arsenal appears to be Cobalt Strike. Most of the examples in the docs appear to be direct commands for its shell or instructions for its GUI.

Initial access

Before Conti can begin wreaking havoc inside the network, they have to first breach it and get a foothold. As mentioned before, there is nothing in the documentation that outlines this process; rather, it seems Conti has developed various crawlers and scanners that scour the internet in search for exploitable/breachable servers. These crawlers will either grant them that initial access to a victim network, or mark them as breachable for their operators and affiliates.

⚠ The following list was created from design documents. We are unsure if they are actually implemented.

Service	Crawler logic
Apache Tomcat	Scan for Tomcat servers, and attempt to exploit the cgi-bin vulnerability
Outlook Web Access (OWA)	Internet crawler and credential brute forcer
Remote Desktop Protocol (RDP)	Scan for servers open to RDP from the internet and attempt to brute force login details. It is port agnostic and does not rely on RDP being on TCP 3389.
SQL	Scan websites that have user inputs and attempt to use SQL injection on them
Printers	Scan for printers accessible from the internet and attempt to exploit them using PRET
Mail	Automatic spambot, capable of sending phishing mails from the local mailbox

Lateral movement

Besides the methodology documents, there are additional manuals with concrete examples and guides on implementing lateral movement —— the techniques listed here are aggregated from all of them, ordered by the amount of examples/references to each (in order of most prominent to least):

- Remote Windows Management Instrumentation (WMI) —— used for triggering payloads remotely using /node:.. process call create
    - Interestingly, the attackers sometimes use it to actually trigger a BITS job to download the malware hosted remotely (or on a breached share)
- PSExec —— both the Sysinternals tool itself and its Cobalt Strike implementation are used for remote payload execution
- Remote scheduled task —— using the command line utility SCHTASKS with the /s flag to create a remote task to execute a dropped payload
- WinRM —— this is the built-in code execution method in Cobalt Strike
- EternalBlue —— exploiting a remote code execution vulnerability in SMB
- BlueKeep —— exploiting a remote code execution vulnerability in RDP

Persistency and backdoors

From the leaked chat logs, the only persistence methods we've seen discussed are scheduled tasks. We've added all of the task names and paths that we've seen in the chat logs to our GitHub repository.

Other persistence methods that we've seen explained in one of Conti's manuals include:

- Registry run keys
- Office application startup
- Windows services
- Image file execution options
- WMI event subscription
- AppInit DLLs
- Winlogon userInit
- LSASS notification packages
- Netsh helper DLL

In addition to the above, which are used to launch their beacons/reverse shells, the manuals also mention installing AnyDesk and Atera, as well as changing the RDP port (and enabling it to pass through Windows' firewall) —— all presumably to have another entry point in case communication is lost (their term for this is закреп, which roughly translates to screwed [in place]).

Privilege escalation

Besides the existing local privilege escalation (LPE) tools available in Cobalt Strike, it appears that Conti uses the LPE variant of PrintNightmare to create new local administrators for beacons that run as a regular user.

Credential harvesting

Most of Conti's credential harvesting manuals reference Mimikatz, but their full arsenal includes:

- Mimikatz
    - lsadump
    - dcsync
    - pth

token injection

- Zerologon —— exploiting a netlogon vulnerability to get an authenticated session to the domain controller and reset the krbtgt password

- Kerberoast —— used to crack kerberos service user passwords from service tickets
- Zerologon —— this time used as a Cobalt Strike post exploitation module to acquire a login session to the DC to run dcsync
- Credential stealer —— probably an in-house development; scans the local filesystem for user passwords stored in text files and documents

Defense evasion

Conti has various ways to avoid detection. The primary (and most surprising) one is ensuring that their released tools do not trigger detection in the first place.

Conti's documentation includes evidence that they test their tools and techniques against a number of well-known antiviruses. These include testing that their droppers and injectors don't trigger various antivirus engines. To do this, they use both local machines running the antivirus engines and dyncheck, a platform that allows sample upload and analysis (similar to VirusTotal, though it seems to not be accessible at the moment).

In particular, the attackers are interested in the following antivirus engines:

- Windows Defender
- ESET Nod32
- Avast Home
- Kaspersky Antivirus
- Bitdefender

In addition, Conti has some manuals on shutting down Windows Defender, either by manipulating the host's policy to turn it off, or by killing its service. It seems that special attention is given to the service, likely due to its widespread usage in target organizations.

The persistent backdoor gets command and control addresses from obfuscated methods, which also helps evade detection:

- emercoin dns
- Google cache
- bitcoin transactions

Saving files to the disk is discouraged, and scripts/lolbins are the preferred way of work. Files saved to disk should be hidden using steganography (in pictures or certificate files) or in a way that can be easily listed (registry, file streams).

Mitigations

Since the attack surface is multifaceted, your defense should also be multi-layered —— there is no one solution that can keep you immediately safe and secure. As we can see in the attack methodology, there is a sophisticated process before the first ransomware instance is deployed, which gives us plenty of opportunity to detect and respond to the attack.

For a correlation between attack method and its mitigation, please refer to Summary: Conti's toolkit.

Access control and ZeroTrust

Conti relies a lot on existing users and their credentials for lateral movement and access. Enforcing control over who can access what and where, and purposely separating power users from daily activities, can greatly inhibit and slow the lateral movement process. It also allows for much more detection surface.

Segmentation

In addition to controlling user access, you can also control the communication paths. Disabling protocols that can be abused for lateral movement (RPC, RDP, WinRM, SSH, etc) between user endpoints, restricting access to file shares (or disabling them altogether on anything that isn't a fileserver), and limiting access to databases and backup servers can greatly reduce your network attack surface.

For a bit of extra granularity, lateral movement methods that rely on RPC (such as remote WMI, remote scheduled tasks, and psexec) can be also controlled at the operating system level, using RPC filters.

Web application firewall

Before any attack can propagate inside your network, the attacker needs to get a foothold in it. In Conti's cases, their initial access crawlers and vectors include phishing (mail spambot) and exploiting internet-facing services (OWA, SQL injection, Apache Tomcat cgi-bin). In most cases, a good web application firewall should block most attacker attempts to gain that initial foothold in the network.

Software inventory and patch management

Keeping track of what software is installed and where it is installed can help detect unwanted additions. This holds true for Conti's Atera and AnyDesk backdoors, and also for other attacks. (Looking at you, LAPSUS$, with your procexp and ProcessHacker.) In addition, patch management can also keep your chestnuts out of the fire. None of the exploits discussed in this blog are recent; patches were released long ago. Despite this, Conti and other groups have been able to be successful because many servers remain unpatched.

Malware detection — EDR/AV

This is the last line of defense on the machines in the network. A good (and up-to-date) endpoint detection and response (EDR) or antivirus (AV) solution may help detect and block the tools used during the attack. It is a cat-and-mouse game, (as we've seen that Conti tests whether their tools bypass detection), but it's better to have a cat that sometimes catches mice than no cat and a mouse infestation.

Some EDRs today also claim to be able to detect and prevent ransomware heuristically, when it starts encrypting your host. We will not make claims on the efficiency rate of this feature, but it is something to consider.

Conclusion

Although there is still much that is unknown about Conti and other ransomware groups, these documents have given the security community a firsthand look at a cybercriminal organization. This information is invaluable as we continue the fight against them and against ransomware in general.

It has become a bit of a trope to say we need to understand the attacker's point of view, but there is a lot of truth to it. By looking at Conti as a business operation whose go-to-market strategy was leaked, we can act as their competitors in a sense, using their own intellectual property against them.

None of the tools Conti is using are particularly novel. Conti's operators have many tools and methods that they employ to infect and eventually encrypt target networks, but they are all known to us. They're not unique zero-day threats, they're "common knowledge" TTPs that are also employed by red teams everywhere.

Despite this, they still have wide success. "If it ain't broke, don't fix it," as they say. This supports the idea that security teams need to take a hard look at how they're approaching defense. Zero days may make the headlines, but the foundational attacks make the money.

Network domination is the goal. Usually, when discussing ransomware, there's more emphasis on the actual act of encryption. The truth, however, that we wanted to showcase with this post, is that there is a long process that has to occur before any encryption can even begin. This time, our discussion is backed by actual ransomware operator documentation. Considering the ratio between hacking documentation and encryption documentation, it becomes clear that the main issue is with hacking (network breach, lateral movement and propagation, avoiding detection) rather than with just data encryption and exfiltration.

This is actually somewhat of a silver lining. This knowledge demonstrates that the detection surface that we as defenders can employ is much wider than it seems — we just need to reach out and utilize it. Just because these TTPs are not new does not make them trivial — if they were, they wouldn't be used by one of the most successful ransomware groups active today. This documentation and analysis supports that we as a community need to look at ransomware more holistically rather than just at the encryption. By focusing primarily on the encryption aspect of ransomware, we are missing out on a wide detection surface which could be the difference between an incident and a headline.

Summary: Conti's toolkit

We have aggregated the following table of Conti's TTPs and possible mitigation measures for them:

Category	Method	Description	Mitigation
Attack Tools	Cobalt Strike	Commercial remote access tools designed for red teams, but often misused by malware operators	• EDR/AV • Segmentation • Access control
	Trickbot	Trojan spyware	
	PSExec	Free Microsoft tool for remote program execution	
Lateral Movement	Remote WMI	Microsoft administration feature capable of remote program execution	• Segmentation • Access control • RPC filters
	Remote Task Scheduler		
	WinRM	Windows service and protocol for remote host management	
	BlueKeep	A Remote Code Execution vulnerability in Microsoft RDP	• Patch management • Segmentation • Access control
	EternalBlue	A Remote Code Execution vulnerability in Microsoft SMB	
Privilege Escalation	PrintNightmare	A Remote Code Execution vulnerability in the Window Print Spooler service	• Patch management
Credential Harvest	Mimikatz	Open source credential dumper	• EDR/AV
	ZeroLogon	An Elevation of Privilege vulnerability in MS-NRPC	• Patch management • Segmentation • Access control • RPC filters
Backdoor	AnyDesk, Atera	Remote access software	• Software inventory management
	Webshells	Dropping webshells on breached web servers	• EDR/AV
	RDP	Windows remote desktop protocol	• Segmentation • Access control
	Persistency techniques	Various persistency methods to load a bot/dropper	• EDR/AV
Detection Avoidance	Disabling Windows Defender	Disabling the antivirus to prevent malware detection	• EDR/AV

		• Software inventory management
[Obfuscation]	Encoding C2 addresses and communication to inhibit detection	• EDR/AV • IDS
Outlook Web Access ([OWA])	Brute forcing access to Outlook web interface to spread phishing emails	• Web application firewall
[RDP]	Brute forcing access to internet-facing servers with RDP open	• Segmentation • Access control
[SQL]	Attempting SQL injection on websites with user input	• EDR/AV • IDS • Web application firewall
Initial Access		
[Printers]	Using exploit kits on printers open to the internet	• Patch management • Segmentation • Access control
[Apache Tomcat Scanner]	Attempting to exploit Apache Tomcat servers	• Web application firewall
[Mail]	Using a spambot to spread phishing emails on compromised mailboxes/hosts	• EDR/AV

References

Although we read all of the documentation files from the leak, some files contained more information than others. We've listed all files that contain the information that was used to write this blog post. We follow the folder tree from [vx-underground].

- Conti Toolkit Leak/
  - Мануали для работяг и софт/
    - MANUALS/
      - МАНУАЛ.txt
      - Заменяем sorted адфиндера.txt
      - ПРОСТАВЛЕНИЕ.txt
      - Меняем RDP порт.txt
      - по отключению дефендера.txt
      - ПЕРВОНАЧАЛЬНЫЕ ДЕЙСТВИЯ.txt
    - CobaltStrike MANUAL_V2 .docx

- Conti Documentation Leak/
    - docs/
        - modules/
            - ТЗ доработка модуля распространения.txt
            - ТЗ автоматизация чистки.txt
            - требования к лоадеру.txt
            - ТЗ бэкдор.txt
            - сканер apache tomcat.txt
            - ТЗ брут OWA.txt
            - ТЗ сканер rdp.txt
            - ТЗ сканер sql инъекций2.txt
            - ТЗ сканер принтеров.txt
            - ТЗ спамбот.txt
        - misc/
            - ТЗ автоматизация группового тестирования в криптопанели.txt
        - management/
            - чистка AB.txt
        - быстрый старт хакера.txt
- Security

Share

Written by

Stiv Kupchik

April 05, 2022

Senior Security Researcher, based in Tel Aviv, IL