Conti Ransomware in Taiwan

By CyCraft Technology Corp

Published: 2021-06-24 · Archived: 2026-04-05 17:52:31 UTC

Conti Ransomware Background

Conti Ransomware was first observed in December 2019 and has been primarily targeting corporate networks since.

Conti is reported to have targeted the following industries:

> *Financial Institutions*
> *Education*
> *Private Organizations*
> *Government Agencies*
> *Healthcare*
> *Small-Sized Enterprises*
> *Medium-Sized Enterprises*

Some of the more interesting aspects of Conti ransomware include:

- Its numerous features and functions not typically seen in other ransomware families
- Its ability to scan and encrypt files from a separate system
- Simultaneously using 32 threads to encrypt files quickly
- Its ability to stop over 140 Windows processes, including processes related to SQL databases

- Its ability to abuse Windows Restart Manager to cleanly close applications to ensure targeted files for encryption aren't locked by said applications
- Deploying up to 277 different algorithms to encrypt different strings, using a unique symmetric encryption key per file, which is then itself encrypted using AES-256 with a bundled RSA-4096 public encryption key.

However, perhaps Conti's most interesting aspect is its similar code snippets, Trickbot distribution, and overlapped infrastructure with Ryuk ransomware, which has some analysts regarding Conti as the successor for Ryuk. Indeed, the number of similarities, combined with the decrease in the use of Ryuk while the use of Conti increases, has some analysts speculating that both Ryuk and Conti share members of the same development/distribution team.

Conti Ransomware in Taiwan

Last year, during a post-breach Incident Response (DFIR) investigation, CyCraft observed and analyzed the effects of a Conti ransomware attack.

Press enter or click to view image in full size

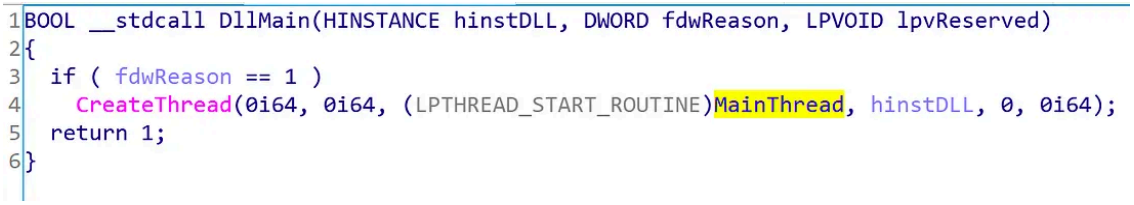
CyCraft Research utilized both manual and automatic tools, as well as open-source tools, to perform semi-autonomous analyses of the encountered Conti Ransomware and its obfuscation techniques.

While our MDR systems can automatically collect behavior activities, manual reverse engineering is sometimes necessary to complement or to verify the monitored behavior activities. In order to improve the performance of manual reverse engineering, several semi-auto mechanisms were implemented.

In our report, we go through each of the more intriguing obfuscation techniques we observed in more granular detail, including:

> *Instrumentation*
> *API Unhooking*
> *Junk Code Inserted*
> *API Resolving By Name Hash*
> *Strings Obfuscation*

Press enter or click to view image in full size



```
BOOL __stdcall DllMain(HINSTANCE hinstDLL, DWORD fdwReason, LPVOID lpvReserved)
{
  if ( fdwReason == 1 )
    CreateThread(0i64, 0i64, (LPTHREAD_START_ROUTINE)MainThread, hinstDLL, 0, 0i64);
  return 1;
}
```

Conti first created a MainThread in DllMain.

Other Observed Tactics & Techniques

One of the trends we have seen with Conti ransomware attacks is the use of double extortion. The threat actor behind this Conti-focused attack not only used encryption for extortion but also threatened to release the victims' data via a data leak site as part of their extortion strategy — most likely to coerce the victims into paying the ransom faster.

Conti ransomware also provided its handler backdoor utility for manual operation — a key feature of Conti and often suggests a highly sophisticated, targeted operation, which not only closely resembles an APT attack but also suggests that the attackers at the helm spent the due diligence on performing detailed reconnaissance prior to launching the attack.

Get CyCraft Technology Corp's stories in your inbox

Join Medium for free to get updates from this writer.

Remember me for faster sign in

Manual operation of ransomware allows for the attackers to configure the ransomware according to the situation and launch when the largest number of endpoints could be compromised.

Basic File Information

In this incident, basic information about the malware we observed in the wild is listed below.

```
filename: wwarc64.dll
md5: eb3fbab995fe3d4c57d4859f1268876c
sha1: 68fe03eb79f5813dccb006699dd1f468b32a4d9esha256: 5c278c04bb19196dc8559d45b9728b3ba0c1bc5cdd20a7
pdb_path: A:\source\conti_v3\x64\Release\cryptor_dll.pdb
```

Extension List 1

```
.4dd, .4dl, .accdb, .accdc, .accde, .accdr, .accdt, .accft, .adb, .ade, .adf, .adp, .arc, .ora, .alf
.db-shm, .db-wal, .db3, .dbc, .dbf, .dbs, .dbt, .dbv, .dbx, .dcb, .dct, .dcx, .ddl, .dlis, .dp1, .dq
```

Extension List 2 (VM / disk image)

Files with the following extensions will use different encryption algorithms.

```
.vdi, .vhd, .vmdk, .pvm, .vmem, .vmsn, .vmsd, .nvram, .vmx, .raw,
.qcow2, .subvol, .bin, .vsv, .avhd, .vmrs, .vhdx, .avdx, .vmcx, .iso
```

Skip Path List

If the path contains the following string (ignorecase), it will be ignored.

```
tmp, winnt, temp, thumb, $Recycle.Bin, $RECYCLE.BIN,
System Volume Information, Boot, Windows, Trend Micro
```

Skip Name List

```
.exe, .dll, .lnk, .sys, .msi, readme.txt, CONTI_LOG.txt
```

Differences With Carbon Black Case

Shadowcopy Deletion. The Conti ransomware we observed had an extremely busy and loud methodology for stopping services and inhibiting recovery on the local system. While many ransomware families will simply delete the Windows Volume Shadow Copies using vssadmin, the Conti we observed used vssadmin in unique ways to ensure their deletion, as shown below.

> *vssadmin Delete Shadows /all /quiet*
> *vssadmin resize shadowstorage /for=c: /on=c: /maxsize=401MB*
> *vssadmin resize shadowstorage /for=c: /on=c: /maxsize=unbounded*
> *vssadmin resize shadowstorage /for=d: /on=d: /maxsize=401MB*
> *vssadmin resize shadowstorage /for=d: /on=d: /maxsize=unbounded*

This newer version of Conti used WMIC to enumerate and delete shadow copy.

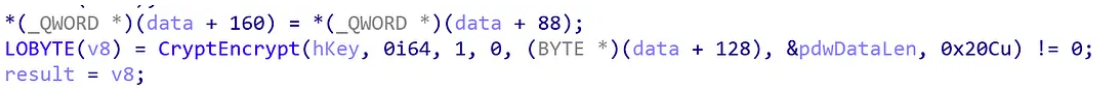
Recommended Mitigations

- Increase and maintain your capability of threat hunting and threat intelligence. While compromised endpoints cannot be avoided, threat hunting with up-to-date intelligence can expose attackers lurking in

your environment before they launch a ransomware attack. Targeted ransomware attacks typically spend more time on recon, penetration, and persistence. Regular threat hunting increases your chances of disrupting the attack before the attackers initiate actions on their final objectives.

- Define and ready your strategy and playbook against ransomware. There is a strong likelihood that Ransomware will eventually land on some of your endpoints. Many response options to ransomware exist for defenders: routine backups, shutting down devices, hibernation, network isolation. Each one has benefits; one solution on its own is not enough. Lastly, estimate the impact on your business with leadership, ensure that you have consistent messaging across all departments, and perform red, blue, and purple team exercises as needed.
- Establish and maintain routine AD security. In our observations, ransomware families typically do not launch the ransomware in the early stages of the attack. Attackers tend to lurk and hunt in your environment. Upon harvesting the AD admin, they immediately start spreading ransomware to every device in your domain at once. Maintaining effective AD security is complicated and hard to manage. The earlier defenders establish playbooks, the earlier they can identify risks and holes in their defenses — both technological and operational.

Press enter or click to view image in full size



Generated Key Encryption

Everything Starts From Security

CyCraft Customers can prevent cyber intrusions from escalating into business-altering incidents. From endpoint to network, from investigation to blocking, from in-house to cloud, CyCraft AIR covers all aspects required to provide small, medium, and large organizations with the proactive, intelligent, and adaptable security solutions needed to defend from all manner of modern security threats with real-time protection and visibility across the organization.

Engage with CyCraft

Blog | LinkedIn | Twitter | Facebook | CyCraft

Press enter or click to view image in full size

CyCraft secures government agencies, police and defense organizations, Fortune Global 500 firms, top banks and financial institutions, critical infrastructure, airlines, telecommunications, hi-tech firms, SMEs, and more by being Fast / Accurate / Simple / Thorough.

CyCraft powers SOCs using innovative AI-driven technology to automate information security protection with built-in advanced managed detection and response (MDR), global cyber threat intelligence (CTI), smart threat intelligence gateway (TIG) and network detection and response (NDR), security operations center (SOC) operations software, auto-generated incident response (IR) reports, enterprise-wide Health Check (Compromise Assessment, CA), and Secure From Home services. Everything Starts From Security.

Meet your cyber defense needs in the 2020s by engaging with CyCraft at engage@cycraft.com

Additional Resources

- Read our latest white paper to learn what threat actors target Taiwan, their motivations & how Taiwan organizations retain resilience against some of the most sophisticated and aggressive cyber attacks in the world.
- Is your SOC prepared for the next decade of cyber attacks? Read our latest report on building effective SOCs in the 2020s, the challenges to overcome, and the stressors to avoid — includes research from Gartner, Inc. on why Midsize enterprises are embracing MDR providers.
- New to the MITRE Engenuity ATT&CK Evaluations? START HERE for a fast, accurate, simple, thorough introductory guide to understanding the results.
- Our CyCraft AIR security platform achieved 96.15% Signal-to-Noise Ratio with zero configuration changes and zero delayed detections straight out-of-the-box.
