


China-Linked Threat Group Targets Taiwan Critical Infrastructure, Smokescreen Ransomware

 medium.com/cycraft/china-linked-threat-group-targets-taiwan-critical-infrastructure-smokescreen-ransomware-c2a155aa53d5

CyCraft Technology Corp

February 21, 2022



[CyCraft Technology Corp](#)

Jun 2, 2021

.

10 min read



The worldwide pandemic did not slow down malicious cyber activity; it fueled it. As early as February 2020, we began observing an increase in malicious activity. In April, one of the largest cyber attacks targeting Taiwan in 2020 was the targeted attack on the CPC Corporation — a state-owned petroleum, natural gas, and gasoline company and the largest gasoline supplier in Taiwan with roughly 25% of the gas stations on the island nation.

CPC Corporation wasn't alone; ten more organizations in critical infrastructure were also targeted for attack that exact same weekend.

Incident Overview

On May 4, multiple CPC (台灣中油股份有限公司) gas stations across Taiwan suddenly became unable to accept payment by CPC VIP cards or electronic transaction apps. Customers had to pay in cash or by credit card until the payment system was up again.



Fig. A —

In the beginning, the state-run CPC denied allegations of being hacked and having their systems compromised. In truth, the CPC had been the victim of a targeted ColdLock ransomware attack.

On May 15, (ten days after the CPC incident), the Investigation Bureau of the Ministry of Justice (MJIB) released an investigation report stating that the CPC was one of more than ten victims in this sophisticated and organized ColdLock ransomware attack. The unnamed ten included

other organizations in Taiwan's critical infrastructure, even a large multinational semiconductor vendor.



Fig. B —

CPC Corporation is not our customer; however, we were involved in investigations regarding other critical infrastructure (CI) victims of the attack's unnamed ten.

This successful, sophisticated attack targeted CI on a national scale, denied service across the country, interrupted the daily life of the common citizen, and brought brief but significant economic turmoil.

Incident Timeline

This timeline was constructed by combining the findings from our own investigation and an analysis of the threat intelligence presented in the MJIB report.



Fig. C — CPC Incident Timeline

Prior to April 26 — The attackers gain initial access and escalate privileges. They have decided (or planned) to wait before acting on their objectives.

April 26 — The attackers initiate their attack just before midnight.

April 27 — The first backdoor is installed.

April 28 & 30 — While the attackers were not directly active in the victim's environment on these days, GPO was leveraged by the attackers to automate the distribution of the ransomware throughout the entire system from April 28 to the day of the attack.

April 29 — The second backdoor is installed under a different file with the same name but with a different hash. This second backdoor becomes the main backdoor used in the operation.

May 1 to 3 — Extended holiday weekends, like the Labor Day holiday weekend, are generally considered an ideal time for cyberattacks as most technicians or security analysts would be on vacation, increasing both detection and response time. The Labor Day holiday weekend was, unfortunately, an ideal time for GPO to automate the distribution of the ransomware throughout the entire system, maximizing the number of affected endpoints for the day of the attack.

May 4 — CPC initially claims a mere system crash; however, as talks of ransomware quickly begin to surface, CPC admits to being victim to a ransomware attack. As CPC is considered critical infrastructure for the country, citizens are gravely concerned about the CPC attack. However, unbeknown to the general public, several other organizations had been targeted as well.

May 4 to 6 — The attackers launch attacks against their other intended targets one after another. Their attack procedure remains the same; backdoors are installed before midnight, GPO distributes the ransomware throughout the targeted system, and the ransomware begins encrypting and deleting data just after 12 noon of the following day.

May 6 — Chunghwa Telecom announces it has been breached and releases IoCs and other relevant threat intelligence. Chunghwa Telecom is the largest telecommunications company and the incumbent local exchange carrier of PSTN, Mobile, and broadband services in Taiwan. Their report is the first report of this operation that contained IOCs, which were later used to attribute the same threat actor for the attacks on Chunghwa Telecom, CPC, and our customer.

May 7 — The malware has been contained and eradicated; the CPC system begins operations without further incident. Our future customer, who had not yet contacted us, follows their post-intrusion playbook policies and begins performing clean reinstalls on all their endpoints.

May 15 — The MJIB issues both a press release and threat intelligence report of the CPC attack.

System-Level Threat Hunting

The initial automated environment scan of our customer's environment, which consisted of 7 thousand endpoints and 382.9 million files, immediately identified 4 suspicious endpoints and 3 suspicious files as a severe threat to the environment. Level 10 threats (as were these) are considered by the CyCraft AIR platform as the most malicious threats an environment could possibly face.

All information in this blog and our report has gone through de-identification and anonymization.



Fig. D — Screenshot of CyCraft AIR’s automated report of our customer’s environment — allowing our human security analyst teams to then focus and drill down into specific queries. All information in this blog and our report has gone through de-identification and anonymization.

Findings

By referencing the published threat intelligence from both Chunghwa Telecom and the MJIB with the intelligence from our own investigation, we concluded that our customer was also targeted by the same threat actors behind both the CPC and Chunghwa Telecom attacks.

When our investigation began, all AD servers had already had a clean reinstall of their OS; however, three system admin endpoints (JOHN706_NB, MIS201_NB, MIS312_NB) still contained artifacts, including backdoors that were still connected to malicious C2 servers (64[.]64.234.24 and 104[.]233.224.227).

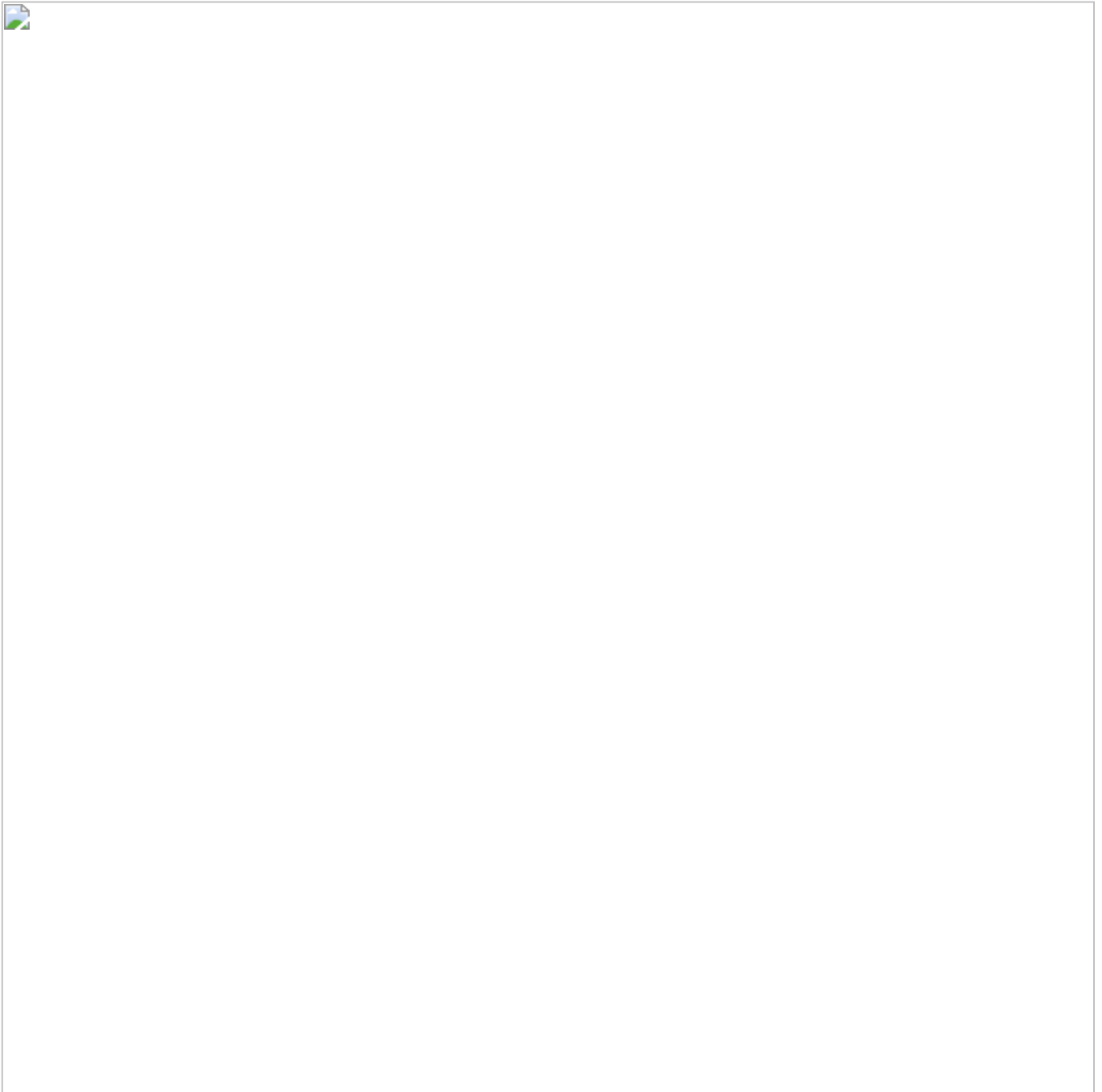


Fig. E — CyCraft AIR Cyber Situation Graph

The backdoor malware (CDPSSVC.DLL) discovered in the system admin endpoint had the exact same hash as the one in the Chunghwa Telecom IoC Report.



Fig. F — CyCraft AIR screenshot of known malware found on customer endpoint
The two IP addresses (64.[.]64.234.24 and 104.[.]233.224.227) were also both listed as malicious C2 servers in the Chunghwa Telecom IoC Report.

Further investigation into the system admin endpoint, MIS201_NB, revealed CobaltStrike Beacon malware that had both identical malware hashes and C2 addresses as those listed in the Chunghwa Telecom.

Actions on Objectives

The attackers had gained high-privileged access into the target system at least one week prior to the attack; however, there is a strong likelihood the target system had been compromised even months before May 4.

The attackers had scheduled the backdoor malware, dewm.exe and qwins5.exe, to be installed on the system admin endpoints at precisely 11:46 p.m. on April 26 and 12:00 a.m. on April 27.



Fig. G — CyCraft AIR cyber situation graph of malicious (pink) processes. Notice the time stamp on each malicious process.

73 minutes later, at 1:01 a.m. on April 27, the attackers acted again and installed the main backdoor program (CDPSSVC.DLL) onto the system admin endpoint. Fig. H shows that in addition to install.bat, the attackers also issued several more commands. Unfortunately, only

CDPSSVC.DLL remained on the endpoint we investigated as the other files had been removed by the previously mentioned clean reinstall.

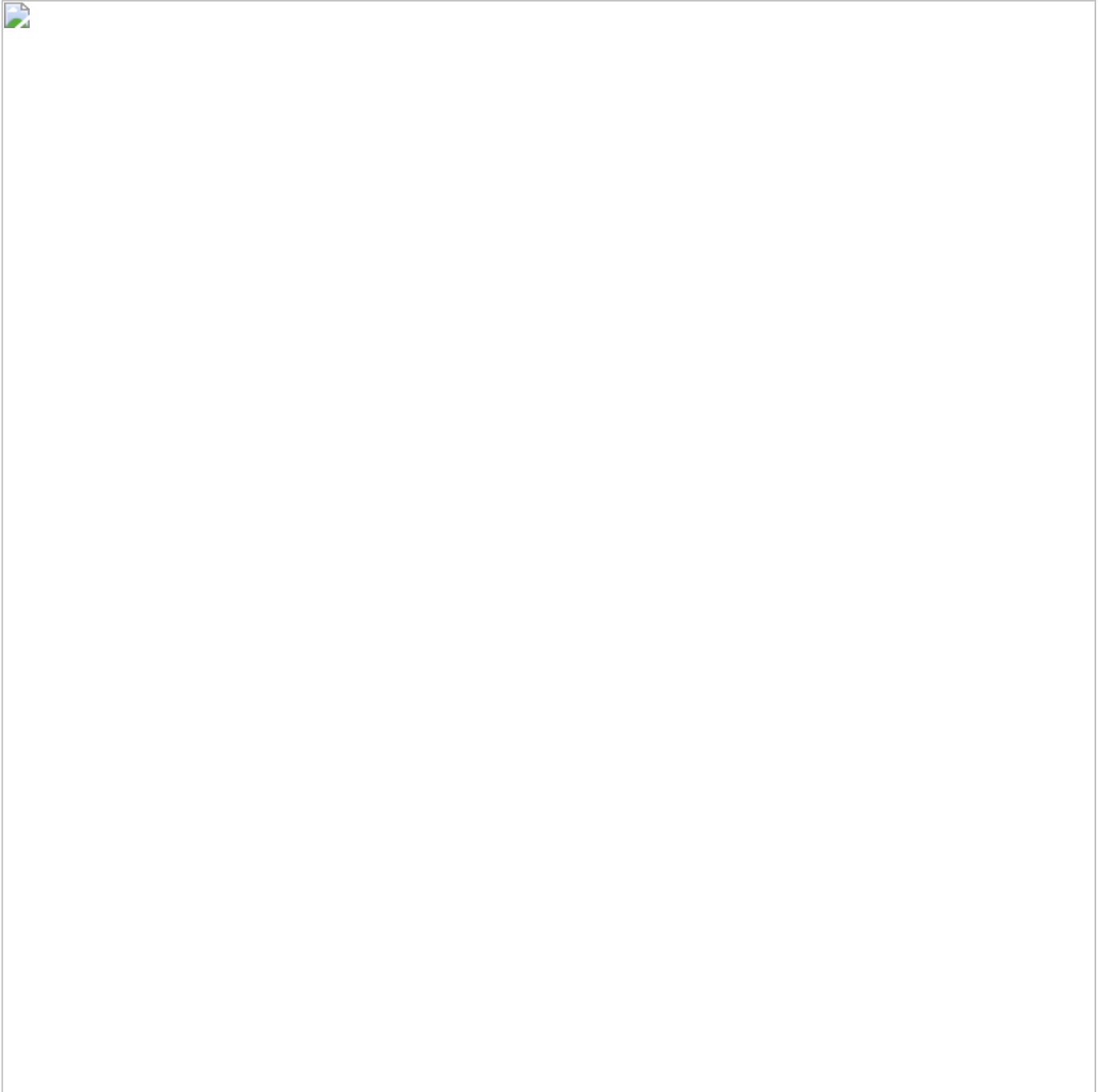


Fig. H — CyCraft AIR cyber situation graph — endpoint process tree

In this process tree (Fig. H), the attackers use “reg add” to add a registry in the services called CDPSSvc and install service by the “sc create” command.



Fig. J — CyCraft AIR cyber situation graph — endpoint process tree

It's important to note that the backdoor malware and the ransomware are separate. A few moments after installing the main backdoor malware, at 1:01 a.m. on Monday, April 27, the attackers used the GPO to distribute the ransomware throughout the entire system over the next three business days and the 3-day Labor Day weekend. The ransomware then laid dormant and activated on Tuesday, May 5.



Fig. K — Ic.tmp PowerShell attacks executing CodeLock ransomware

Although the ransomware started execution when the host endpoint was booted up on May 4, the ransomware waited until 12:10 p.m. (Tuesday, May 5) to begin encrypting files and destroying data. There are several reasons for this scheduled delay: it would be difficult for engineers and security analysts to respond immediately at this time, and it was the second day back after a long weekend.



Fig. L — Encryption and Deletion did not begin until 12:10 in the afternoon.

A closer look into the malware revealed this particular variant of ColdLock had removed all the payment information, contact email, and the RSA public key. This indicates that no information could be provided for decryption.

Ransomware-as-a-Smokescreen

Ransomware incidents have dramatically increased in frequency, severity, and complexity ever since the release of Bitcoin in 2009 as well as the numerous other cryptocurrencies that followed. This consistent and dramatic rise suggests that ransomware does work and attackers do get paid.

However, ransomware's increase in media and academic coverage has led to a relatively recent development. Ransomware has become notorious enough that attackers have now begun to weaponize the fear of ransomware, employing ransomware as a smokescreen for other malicious intents.

In terms of this particular incident, the existence of various versions of this particular ransomware on VirusTotal (VT) and the lack of decrypting messages suggest that the attackers had no intention of providing their victims a means of decrypting their encrypted files — yet another reason why many cybersecurity vendors strongly recommend against paying ransomware.

In addition to the lack of sophistication in the malware used in this attack, specific attacker behavior proved inconsistent with observed behavior in previous ransomware attacks, such as the decision to not delete volume shadow copies, as doing so would dramatically increase the possibility of recovery.

As this attack was also launched just one week before Taiwan's presidential inauguration, targeted multiple organizations in multiple industries, used a lack of sophisticated ransomware, displayed non-optimal attacker behavior, and was attributed to China-linked threat groups by the FBI, the MJIB, and us, it becomes increasingly more likely that the end objective of this attack was not financial gain but political deterrence.

The ransomware was just a smokescreen used to confuse and delay investigators. The attackers had weaponized the fear of ransomware to deceive defenders and achieve their end objectives.

MITRE ATT&CK® Adversarial Technique Mapping

Execution

T1047 Windows Management Instrumentation
T1053.002 Scheduled Task/Job: At (Windows)
T1059.001 Command and Scripting Interpreter: PowerShell
T1106 Native API

Persistence

T1053.002 Scheduled Task/Job: At (Windows)
T1543.003 Create or Modify System Process: Windows Service

Privilege Escalation

T1053.002 Scheduled Task/Job: At (Windows)
T1484 Group Policy Modification
T1543.003 Create or Modify System Process: Windows Service

Defense Evasion

T1070.004 Indicator Removal on Host: File Deletion
T1070.006 Indicator Removal on Host: Timestomp
T1484 Group Policy Modification
T1497.003 Virtualization/Sandbox Evasion: Time Based Evasion
T1562.001 Impair Defenses: Disable or Modify Tools

Discovery

T1007 System Service Discovery
T1033 System Owner/User Discovery
T1049 System Network Connections Discovery
T1082 System Information Discovery
T1083 File and Directory Discovery
T1497.003 Virtualization/Sandbox Evasion: Time Based Evasion

Impact

T1486 Data Encrypted for Impact
T1489 Service Stop

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

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 , 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 , 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? for a fast, accurate, simple, thorough introductory guide to understanding the results.
- Our CyCraft AIR security platform achieved with zero configuration changes and zero delayed detections straight out-of-the-box.