China Implicated in Prolonged Supply Chain Attack Targeting Taiwan Financial Sector

medium.com/cycraft/china-implicated-in-prolonged-supply-chain-attack-targeting-taiwan-financial-sector-264b6a1c3525

CyCraft Technology Corp

February 23, 2022

CyCraft Technology Corp

Feb 22

·

6 min read

Severe Vulnerability Uncovered in Major Taiwan Financial Software

Taipei, Taiwan — 22 February 2022 — CyCraft, a leading managed detection and response (MDR) provider based in Taiwan, uncovered intelligence regarding the November 2021 cyberattacks targeting the Taiwan financial and securities trading sector; CyCraft further attributed the cyberattacks to — a China state-sponsored hacker group widely believed to be associated with the Chinese Intelligence Agency, the **.**

The November 2021 attacks were originally attributed to password mismanagement; however, following a security incident response (IR) investigation conducted by CyCraft into the second wave of February 2022 attacks, new evidence uncovered the exploitation of a severe vulnerability in commonly used financial software aided by a newly identified hacking technique, **.**

These attacks are the latest in a series of attack campaigns against Taiwan by China-based threat groups. In early 2020, CyCraft curtailed a year-long attack campaign targeting Taiwan's semiconductor ecosystem; this attack was attributed to another China-based threat group, Chimera. Again, in April 2020, a CyCraft incident response (IR) investigation into a government agency breach uncovered Waterbear malware — malware designed and distributed by the China-based threat group BlackTech.

The frequency of cyberattacks targeting Taiwan institutions surged by 38% in 2021, reaching an average of 2,644 attacks per week, Taiwan News reports. The global average is 925 attacks per week. This disparity is due to Taiwan's unique geopolitical situation, high-tech economy, and mature communications infrastructure.

First Attack Wave, November 2021

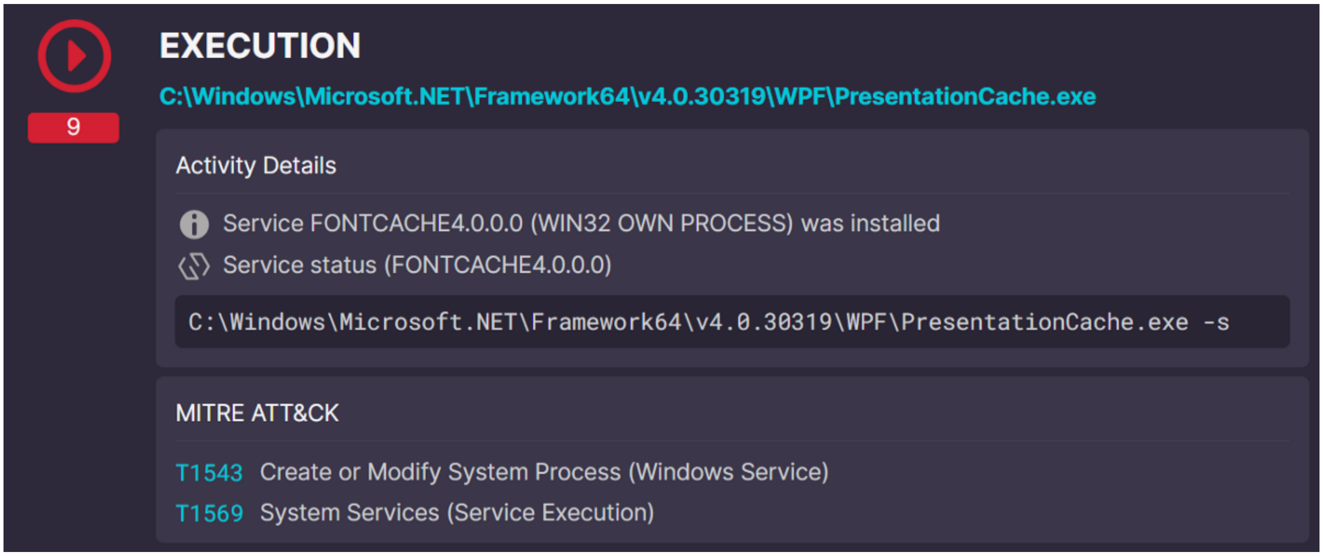
At 5:27 p.m. on Thursday, November 25 of last year, a number of Taiwan financial institutions and securities traders informed the Taiwan Stock Exchange Corporation (TWSE) and the Financial Supervisory Commission (FSC) that they would be suspending online transactions due to suspicious behavior — large, unusual purchases of Hong Kong stocks on consumer trading accounts — as a result of a cyberattack.

After several weeks, the IR investigations theorized that the November attacks were most likely due to password mismanagement and **credential stuffing**; however, the findings were not conclusive and suggested there may have been other causes.

Credential stuffing attacks leverage poor cyber hygiene habits (i.e., users reusing the same username/password combinations across multiple platforms and websites). Several security countermeasures were taken, including forced password updates and multi-factor authentication.

Second Attack Wave, February 2022

Once again, in mid-February 2022, a number of Taiwan financial institutions and securities traders were targeted — some being victims of the November 2021 attacks and others CyCraft customers. CyCraft MDR/EDR cybersecurity solutions observed suspicious files and login events on customer servers and immediately began investigating. **After three days, CyCraft completed their IR investigations**.



EXECUTION

C:\Windows\Microsoft.NET\Framework64\v4.0.30319\WPF\PresentationCache.exe

Activity Details

Service FONTCACHE4.0.0.0 (WIN32 OWN PROCESS) was installed

Service status (FONTCACHE4.0.0.0)

```
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\WPF\PresentationCache.exe -s
```

MITRE ATT&CK

T1543 Create or Modify System Process (Windows Service)

T1569 System Services (Service Execution)

CyCraft MDR's first detection, auto triage, and alert sent for malicious executable PresentationCache[.]exe

CyCraft's three-day IR investigation uncovered that neither the February 2022 nor the November 2021 attacks were solely a direct result of credential stuffing. A more thorough investigation revealed evidence suggesting credential stuffing was purposely left behind by APT10 — credential stuffing was just a smokescreen.

Both attacks were the result of a supply chain attack targeting specific financial software. A vulnerability existing in financial software with a majority market share among Taiwan securities traders was exploited by the attackers, granting them high-level access to multiple firms. Further investigation showed that what was initially presumed to be two separate waves of cyberattacks was actually one prolonged attack campaign in which the attackers leveraged advanced obfuscation techniques not previously observed.

This isn't the first "smokescreen attack" by a China-based threat group. In April 2020, CyCraft observed a China-based threat group use ransomware as a smokescreen for a targeted attack on the CPC Corporation, as reported by CyCraft and Bloomberg.

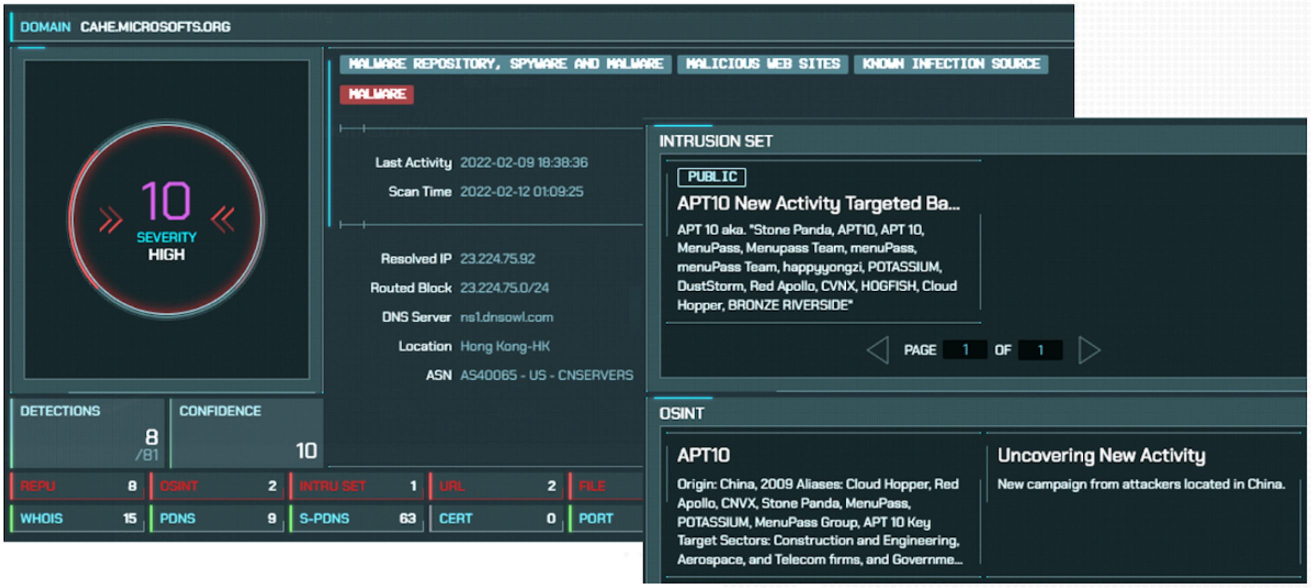
> "For more than a decade, Chinese hackers have waged a persistent cyber offensive against Taiwanese government, non-government and corporate targets. Taiwan also happens to be home to some of the electronics, semiconductor, and military technology that China desperately wants to get its hands on."
> Bloomberg on smokescreen cyberattack targeting the CPC Corporation

Attack Attribution

Analysis of the attacker C2 domain, the Quasar backdoor malware, and the attacker behavior used in the attacks has led to a high degree of confidence in attributing the attacks to a Chinese threat actor. In the second wave of attacks observed by CyCraft, there is a medium degree of confidence in the attribution of APT10 — a China-based threat group.

The objective of these attacks does not appear to have solely been financial gain but rather the exfiltration of brokerage information, the scraping of high-value PII data, damaging the reputation of Taiwan financial institutions, and the disruption of investor confidence during a period of economic growth for Taiwan.

One of the many attack techniques utilized by APT10 was the new technique “Reflective Code Loading”, which was incorporated into the MITRE ATT&CK framework just last October.



DOMAIN CAHE.MICROSOFTS.ORG

Last Activity 2022-02-09 18:38:36
Scan Time 2022-02-12 01:09:25

Resolved IP 23.224.75.92
Routed Block 23.224.75.0/24
DNS Server ns1.dnsowl.com
Location Hong Kong-HK
ASN AS40065 - US - CNSERVERS

DETECTIONS 8 /81
CONFIDENCE 10

REPU	8	OSINT	2	INTRU SET	1	URL	2	FILE
WHOIS	15	PDNS	9	S-PDNS	63	CERT	0	PORT

INTRUSION SET

PUBLIC
APT10 New Activity Targeted Ba...
APT 10 aka. "Stone Panda, APT10, APT 10, MenuPass, Menupass Team, menuPass, menuPass Team, happyyongzi, POTASSIUM, DustStorm, Red Apollo, CVNX, HOGFISH, Cloud Hopper, BRONZE RIVERSIDE"

OSINT

APT10
Origin: China, 2009 Aliases: Cloud Hopper, Red Apollo, CNVX, Stone Panda, MenuPass, POTASSIUM, MenuPass Group, APT 10 Key Target Sectors: Construction and Engineering, Aerospace, and Telecom firms, and Governme...

Uncovering New Activity
New campaign from attackers located in China.

CyberTotal Cyber Threat Intelligence Platform Detecting APT10 Activity

ABOUT APT10

This Advanced Persistent Threat (APT), known as APT10 by MITRE ATT&CK nomenclature, has been active since at least 2006. Common targets of APT10 include healthcare, defense, finance, maritime, biotechnology, energy, and governmental organizations, with an emphasis on targets in Japan and Taiwan. APT10 is believed to be associated with the Chinese Intelligence Agency, the Ministry of State Security (MSS).

In 2018, the U.S. Department of Justice charged two members of APT10, Zhu Hua and Zhang Jianguo, with conspiracy to commit computer intrusions, conspiracy to commit wire fraud, and aggravated identity theft. The Department of Justice charges that these individuals acted in association with the Tianjin State Security Bureau and had been engaging in global computer intrusions for more than a decade.

Three-Day Incident Response

The fast, accurate, and thorough response of CyCraft’s three-day IR investigation is due to their autonomous ML-driven security technology. CyCraft cybersecurity solutions specialize in automated malicious behavior detection and response and are capable of continuously monitoring and managing the cyber situation of even large-scale enterprises with hundreds of thousands of endpoints.

> *“CyCraft strives for human-AI collaboration in cybersecurity. All our solutions — from our dark web intelligence fusion platform, RiskINT, to our endpoint detection and response Xensor agent — are driven by our CyCraft AI Virtual Analyst as well as our team of seasoned human professionals. Not only is the security and safety of the entire CyCraft customer community and their data important to us, but so is creating a frictionless and intuitive user experience that puts all our customers’ cybersecurity concerns at ease. Our technology is complicated; our service isn’t.” — PK Tsung, CyCraft Co-Founder & CSO*

About CyCraft

CyCraft secures government agencies, financial institutions, semiconductor manufacturing, police and defense organizations, Fortune Global 500 firms, airlines, telecommunications, SMEs, and more by being **Fast / Accurate / Simple / Thorough.**

CyCraft automates information security protection with built-in advanced managed detection and response (MDR), global cyber threat intelligence (CTI), smart threat intelligence gateways (TIG), 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. CyCraft also collaborates with other cybersecurity organizations, including the International Forum of Incident Response & Security Teams (FIRST) and the Taiwan Cybersecurity Center of Excellence (CCoE).

Meet your modern cyber defense needs by engaging CyCraft at engage@cycraft.com

Engage with CyCraft

Contacts

Dr. Benson Wu
Co-Founder & CEO, CyCraft Technology
benson.wu@cycraft.com

Chad Duffy
VP of Strategy, CyCraft Technology
chad.duffy@cycraft.com