LuoYu: Continuous Espionage Activities Targeting Japan with the new version of WinDealer in 2021

Leon Chang, Yusuke Niwa, Suguru Ishimaru
Speakers’ Bio

Leon Chang
Malware Researcher @ TeamT5
His major areas of research include APT campaign tracking, malware analysis.

Yusuke Niwa
Cybersecurity Researcher @ ITOCHU Corporation
He tracks threat trends including malspam, APT, and CyberCrime.

Suguru Ishimaru
Malware Researcher @ Kaspersky Lab
He conducts research of the latest threat trends including APT at a global level.
AGENDA

01 Summary of LuoYu campaign in 2021
02 Anatomy of WinDealer
03 Case Studies
04 Conclusions
AGENDA

01 Summary of LuoYu campaign in 2021

02 Anatomy of WinDealer

03 Case Studies

04 Conclusions
Summary of LuoYu campaign in 2021

- The LuoYu Threat Group Overview
- Motivation: Why do we research LuoYu activity?
- Timeline of LuoYu campaign in 2021
- Target regions and industries
  - Subsidiaries of Japanese organizations in China
  - The users of private Chinese bank
The LuoYu Threat Group Overview
The name: 貳魚 (LuoYu)

- 貳魚 (LuoYu) a Chinese mythological creature
- 貳魚，魚身而鳥翼，音如鴛鴦，見則其邑大水。
- Translation: Fish with a pair of wings; When it appears, floods always follow.
LuoYu

Malware
- ReverseWindow
- WinDealer
- SpyDealer
- XDealer
- ShadowPad
- PlugX

Target Industry
- Technology
- Media
- Education
- Financial
- MOFA
- Military
- Telecom
- Logistics

Target Areas
- China
- Hong Kong
- Japan
- Korea
- Taiwan
- Russia
- United State
- Czech Republic
- Australia
- Germany

Origin
- China

New updates
Goal

Attack

Collecting information from dissidents

Attack

Chinese branches of Japanese company

Japan
Timeline of LuoYu Campaign in 2021
Timeline of LuoYu campaign in 2021

**Case 1**
- **Apr. 2021**: Identify new cross-platform backdoor “XDealer”
- **Aug. 2021**: The users of private Chinese bank

**Case 2**
- **Dec. 2021**: Dropper of ReveseWindow & ShadowPad

**Case 3**
- **May. 2021**: Chinese branch of Japanese company

**Case 4**
- **Aug. 2021**: The Linux variant of XDealer
- **Aug. 2021**: Another Chinese branch of Japanese company
AGENDA

01  Summary of LuoYu campaign in 2021
02  Anatomy of WinDealer
03  Case Studies
04  Conclusions
# Malware profile: WinDealer

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type</strong></td>
<td>Modular backdoor</td>
</tr>
<tr>
<td><strong>Naming</strong></td>
<td>string prefix “Deal” in its export function</td>
</tr>
<tr>
<td><strong>First seen</strong></td>
<td>2008</td>
</tr>
<tr>
<td><strong>function</strong></td>
<td>Getting victim label from non-exist URL or non-exist domain</td>
</tr>
</tbody>
</table>
| **C2**     | - C2 config  
              - IP address generation algorithm (IPGA) **NEW** |
| **Linked APT** | LuoYu |
The hardcoded version of WinDealer probably comes from the built date.

Version format: {Main_version}.{year}.{month+day}

We observed four versions from collected samples:

- 16.18.1030
- 17.19.0505
- 18.19.0628
- 18.20.1225 NEW
Hardcoded version of WinDealer

- Before 2016, WinDealer used hardcoded development timestamp string as mutex string
- We use the mutex string prefix to distinguish the backdoor version
  - WORK_20080729400351362402 → WinDealer 2008
  - MANAGE_20130831175600761943 → WinDealer 2013

```c
if ( strstr(Filename, Buffer) || strstr(Filename, SubStr) )
{
    v4 = CreateMutexA(0, 0, "WORK_20080729400351362402");
    if ( v4 )
    {
        if ( GetLastError() == 0xB7 )
            goto LABEL 9;
    }
    v4 = CreateMutexA(0, 0, "MANAGE_20090629400351362402");
    if ( v4 )
    {
        if ( GetLastError() == 0xB7 )
        {
```
Evolution of WinDealer
Evolution of WinDealer

WinDealer 2008
At first, the malware is designed to collect the sensitive data from popular messaging application in China. (support 15 command)

WinDealer 2013
In 2013, it supported more spying function. (support 26 command)
The non-exist URL: "http://www.360.cn/status/getsing.asp"

WinDealer 16.18.1030
Since 2016, There’s hardcore version in WinDealer which contains the feature to steal shadowsocks profile.

WinDealer 17.19.0505
The non-exist URL was changed to "http://www.360.cn/status/getonefile.asp"

WinDealer 18.19.0628
The non-exist URL was changed to non-exist domain: http://www.microsoftcom/status/getsing.asp, 48 command

WinDealer 18.20.1225
The latest version of WinDealer

NEW
In-Depth Analysis of WinDealer
In-Depth Analysis of WinDealer

- Steganography Technique
- Embedded DLL
- Collecting host information
- C2 communications
- WinDealer Related Component
The malware contains an additional module in the resource “Bitmap” using steganography technique to evade security products.

- The encrypted DLL in res ID:129

Md5:76ba5272a17fdab7521ea21a57d23591
Decrypt the embedded DLL

WinDealer EXE

- Encrypted embedded DLL
  - Magic hex (4 bytes)
  - Size (4 bytes)
  - XOR Key (10 bytes)

Encrypted BLOB

- XOR (10 bytes key)
- AES (16 bytes key)

Embedded DLL
How to find BLOB and decrypt

- The search method is to add 0x3000 bytes from the beginning of the image, then advances 1 byte at a time and compares the magic hex pattern to find the desired location.
- The embedded DLL is XORed using the 10 bytes key.
## The functionality of embedded DLL

<table>
<thead>
<tr>
<th>Export function name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>partInitOpt</td>
<td>Mapping embedded functions on VFT for using from main module as initialization</td>
</tr>
<tr>
<td>GetConfigInfo</td>
<td>Mapping embedded malware configuration data from the DLL</td>
</tr>
<tr>
<td>AutoGetSystemInfo</td>
<td>Creating many threads to get infected device information</td>
</tr>
</tbody>
</table>
Generated victim ID set in a reg key

- The victim ID format: MD5("<MAC address><Physical_Drive_info><username>")
- The malware creates a specific registry key to store the generated victim ID to use in the next execution.
- As a unique hidden trick, the victim ID is not stored raw data, the malware converts the 4 bytes victim ID to an IP address style.
Collecting host information

- Computer name
- Username
- CPU info
- OS version
- Network interface
- External IP address
- User account
- Screenshots

```c
char __thiscall get_victim_info_entry(DWORD *this)
{
    getComputerName();
    getUsername(this);
    getCPUinfo(this);
    getOSversion(this);
    getNetworkCard(this);
    TimeZone(this);
    getPublicIP(this);
    if ( this[9] )
        EnumUserInfo(this);
    return 1;
}
```
Before sending the victim data, the malware will add a custom header to the data

- Interesting features:
  - Getting victim label from non-exist domain or non-exist URL based on WinDealer version
    - http://www.360[.]cn/status/getsing.asp
    - http://www.360[.]cn/status/getonefile.asp
    - NXDOMAIN: http://www[.]microsoftcom/status/getsing.asp

- C2 anti-tracking mechanism
  - IP address generation algorithm (IPGA)
Getting victim label from NXDOMAIN

WinDealer
MD5: d9a6725b6a2b38f96974518ec9e361ab

C:\ProgramData\789406d0
1 = 0xB
2 = 0x16
0 = others

Backdoor command 0x60 + headsign: 1

www.microsoft.com

http://www.microsoft.com/status/getsign.asp

111.120.0.0 - 111.123.255.255
113.62.0.0 - 113.63.255.255

IPGA

\x11\x22\x31\x33\x44
C2 anti-tracking mechanism

- Use IPGA (IP Generation Algorithm) to generate a random C2 IP address when backdoor does not have C2 config
- The randomly generated IP will exist within specific IP address ranges
  - Ex: 113.62.0.0 - 113.63.255.255 or 111.120.0.0 - 111.123.255.255
- This mechanism will prevent researchers from tracking down the real C2 IP
C2 communications

WinDealer

Custom header | RSA encrypted | Generated AES Key | TCP/UDP socket

Custom header | AES encrypted | Victim data | TCP/UDP socket

C2 Server
### Data format of c2 communications (first connection)

<table>
<thead>
<tr>
<th>Offset</th>
<th>Description</th>
<th>Example(hex)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x00</td>
<td>Magic header</td>
<td>06 81 DA 91 CE C7 9F 43</td>
</tr>
<tr>
<td>0x08</td>
<td>Generated Victim ID</td>
<td></td>
</tr>
<tr>
<td>0x0C</td>
<td>Victim label</td>
<td>00 or 01 or 02</td>
</tr>
</tbody>
</table>
| 0x0D   | Connection type or Backdoor command ID    | 00 = initial connection
01 = after initial connection
Others = backdoor command ID |
| 0x0E   | Unknown static value                      | 11 or 14                                                                    |
| 0x0F   | Unknown static value                      | 00                                                                           |
| 0x10   | Encrypted data + checksum                 |                                                                              |
Generate 16 bytes AES key to encrypt C2 communication

```
push  14h ; unsigned int
call  operator new(uint)
push  0 ; Time
mov   esi, eax
call  ds:time
add   esp, 8
mov   edi, eax
push  esi ; 0x286AD70
call  GetCurrentThreadId
push  eax ; 0x1CC8
call  GetCurrentProcessId
push  eax ; 0x1E38
push  edi ; 0x613F0C54
lea   eax, [esp+4Ch+buf_str]
push  offset aUUUX ; "%u%u%u%u"
push  eax ; Buffer
call  ds:printf ; ret. 02EFFA0C = "1631521876773673682b6ad70"
lea   ecx, [esp+54h+buf_str] ; "1631521876773673682b6ad70"
push  eax ; size
push  ecx ; buf_str = "1631521876773673682b6ad70"
push  offset aes_key
call  md5_40B5C0 ; ret. aes_key =
        0041EB40 62 EE BC 0D 65 E4 D7 9D C4 CF 06 6E 64 B7 05 37
```
Sending AES key crypted RSA
C2 communication encrypted by AES
1 byte command in custom header+0xD
Divided backdoor in EXE and Embedded DLL

PPTV(pplive)_forap_1084_9993.exe
We have found the downloader of WinDealer in the wild since 2013.

In addition, we found old Windows kernel module downloader (2015 ~ 2017)

- PDB string: “Z:\¥植入相关¥本地溢出¥downexecdriver¥bin¥FAT32.pdb”
We discovered a WinDealer downloader which contains a legitimate domain but the URL path is non-existing. (DNS hijacking or network hijacking)

- User-agent is an unique "BBB," which also appears in WinDealer RAT.
There’re multiple dropper/loader samples related to WinDealer.

The malware resource “AAA” contains an encrypted payload
- The encrypted payload in res ID:103

Ex. The malware uses XOR to decrypt the payload, then loads the decrypted payload (WinDealer) in-memory.
AGENDA

01 Summary of LuoYu campaign in 2021
02 Anatomy of WinDealer
03 Case Studies
04 Conclusions
Case Study 1: Fake site and app

- Phishing site and trojanized installer impersonate private Chinese online banking app
Case Study 2: Drop error image for distraction

The dropper of ReverseWindow (.error.exe)

Drop & Execute

Drop & Execute

Delete dropper

Drop & Open Directory

ReverseWindow version: 2.2.2006131

Connect

C2 Server

Bash Script
(C:\ProgramData\u.bat)

Decoy (\Error.jpg)

Deceive & Distract
Recently, we found that LuoYu is using Shadowpad to attack unknown targets. Case Study 2: Combine use of both proprietary and shared backdoors.

- ReverseWindow version: 2.2.2006131
- ShadowPad latest obfuscation method (code scattering)

C2 Server ➔ ReverseWindow ➔ ShadowPad ➔ Unknown target
Case Study 3

TIM (a legitimate communication tool) tried to download the WinDealer, qbupd.exe somehow even though accessing a legitimate destination of updater.

C:¥Users¥<UserName>¥AppData¥Roaming¥Microsoft¥Windows ¥Start Menu¥Programs¥Startup¥qbupd.exe

After created WinDealer on the startup folder, once victim user logged in this host, WinDealer is executed and sends stolen data over 6999/UDP to backbone router.
YoudaoDict (legitimate tool) tried to download the WinDealer, version.dll, then dll-sideloaded it and executed embedded dll at the end of June 2021.

AV has detected this version’s WinDealer several times though, due to the replacement of AV in this organization, the victim host resulted in compromised.
Public info research (Chinese BBS)

Chinese blog post from Feb 2019 describes a WinDealer-related infection and involving an executable with the same file name (`pptv(pplive)_forap_1084_9993.exe`) which we’ve observed.
Details of Infection flow

- Legitimate EXE downloads a WinDealer in the specific conditions.

Code snippet:
```
.loc_402D16:
    ; CODE XREF: WinMain(x,x,x)+162↑j
    ; WinMain(x,x,x)+1A2↑j
    mov    [ebp+String1], offset download_src ; "http://download.pplive.com/PPTV(pplive)"...
    mov    eax, [ebp+String1] ; http://download.pplive.com/PPTV(pplive)_forap_1084_9993.exe
    push   eax
    push   offset aLoaderPszurlS ; "[Loader] pszUrl:%s"
    push   offset unk_4091C8 ; this
    call   ?Format@CString@@QAAXPBDOZZ ; CString::Format(char const *,...)```

Update request:
http://download.pplive.com/PPTV(pplive)_forap_1084_9993.exe

Only specific conditions
WinDealer’s Initial Vector & Communication Flow

Initial Vector
- Victim Host with a legitimate tool and its updater
- Legitimate Apps
- Backbone Router (CN)
- Legitimate Update Server
- LuoYu’s C2

LuoYu

Post Exploitation
- Infected victim host with WinDealer
- WinDealer or Dropper

Step 1: query a non-exist domain for labeling victims
Step 2: send victim data to backbone router by IPGA

Malware hosted Server

Invisible Area
AGENDA

01 Summary of LuoYu campaign in 2021
02 Anatomy of WinDealer
03 Case Studies
04 Conclusions
LuoYu campaign in 2021

**CAPABILITY**
- SIGINT Technique (N/A)
- Manipulating a legitimate software
- Update mechanism
- Leverage IPGA
- Usage of DLL-Sideloading
- Send stolen data with UDP protocol

**ADVERSARY**
- LuoYu: Chinese-speaking actor
- Possible collaboration with the other Chinese APT group

**TARGET**
- Target area: Wide range, mainly East Asia (including Chinese branches of Japanese companies)
- Target industries: Wide range

**INFRASTRUCTURE**
- CHINANET-BACKBONE 113.62.0.0/15 or 111.120.0.0/14 (random IP addresses)
## LuoYu’s TTPs
### MITRE ATT&CK Mapping

<table>
<thead>
<tr>
<th>Tactics</th>
<th>Techniques</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial Access</td>
<td><strong>T1199</strong> Trusted Relationship: Leverage SIGINT to tamper with traffic at the ISP level</td>
</tr>
<tr>
<td>Execution</td>
<td><strong>T1059.003</strong> Command and Scripting Interpreter: Windows Command Shell</td>
</tr>
<tr>
<td></td>
<td>WinDealer creates a pipe with <code>cmd.exe</code></td>
</tr>
<tr>
<td>Persistence</td>
<td><strong>T1547.001</strong> Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder</td>
</tr>
<tr>
<td></td>
<td>WinDealer sets a value in the registry</td>
</tr>
<tr>
<td></td>
<td>“HKEY_CURRENT_USER\Software\Microsoft\Windows\Currentversion\Run” for startup.</td>
</tr>
<tr>
<td></td>
<td>WinDealer has been created on startup folder below.</td>
</tr>
<tr>
<td></td>
<td>C:\Users&lt;UserName&gt;\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\qbupd.exe</td>
</tr>
<tr>
<td>Defense Evasion</td>
<td><strong>T1027.002</strong> Obfuscated Files or Information: Software Packing</td>
</tr>
<tr>
<td></td>
<td>WinDealer’s functions are divided between the EXE and DLL. The DLL is implemented in its own resource with encryption. Hardcoded strings / data are obfuscated in some WinDealer samples. Gathered data is XORed using a one-byte key “Y”.</td>
</tr>
<tr>
<td></td>
<td><strong>T1574.002</strong> Hijack Execution Flow: DLL Side-Loading:</td>
</tr>
<tr>
<td></td>
<td>WinDealer is executed DLL Side-loading by legitimate PE files</td>
</tr>
<tr>
<td>Tactic</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>T1012</td>
<td><strong>Query Registry:</strong> WinDealer lists installed applications and stores configuration information in the registry.</td>
</tr>
<tr>
<td>T1016</td>
<td><strong>System Network Configuration Discovery:</strong> WinDealer lists networks adapters and their addresses</td>
</tr>
<tr>
<td>T1016.001</td>
<td><strong>System Network Configuration Discovery:</strong> Internet Connection Discovery WinDealer gets the public IP via “<a href="http://icanhazip.com/%E2%80%9D">http://icanhazip.com/”</a>.</td>
</tr>
<tr>
<td>T1049</td>
<td><strong>System Network Connections Discovery:</strong> WinDealer scans the hosts in the LAN using ICMP.</td>
</tr>
<tr>
<td>T1057</td>
<td><strong>Process Discovery:</strong> WinDealer gets the process list.</td>
</tr>
<tr>
<td>T1082</td>
<td><strong>System Information Discovery:</strong> WinDealer gets hostname, CPU info, OS version, mac address and username. The backdoor command 0xD obtains the keyboard layout.</td>
</tr>
<tr>
<td>T1083</td>
<td><strong>File and Directory Discovery:</strong> WinDealer gets a file list and metadata of specified files.</td>
</tr>
<tr>
<td>T1120</td>
<td><strong>Peripheral Device Discovery:</strong> WinDealer gets system disk information and USB drive information.</td>
</tr>
<tr>
<td>T1518</td>
<td><strong>Software Discovery:</strong> WinDealer lists installed applications, WinDealer gets configuration files of chat applications such as Skype, QQ, WeChat and wangwang.</td>
</tr>
</tbody>
</table>
LuoYu’s TTPs
MITRE ATT&CK Mapping

<table>
<thead>
<tr>
<th>Tactics</th>
<th>Techniques</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collection</td>
<td>T1113 <strong>Screen Capture:</strong> WinDealer can take screen captures.</td>
</tr>
<tr>
<td>Command and Control</td>
<td>T1568 <strong>Dynamic Resolution:</strong> WinDealer dynamically generates C2 IP using IPGA.</td>
</tr>
</tbody>
</table>
|                    | T1573.001 **Encrypted Channel:** Symmetric Cryptography  
                            Further communications are encrypted by AES-128 in ECB mode. |
|                    | T1573.002 **Encrypted Channel:** Asymmetric Cryptography  
                            WinDealer uses RSA-2048 during its key exchange phase. |
| Exfiltration       | T1041 **Exfiltration Over C2 Channel:** WinDealer exfiltrates the gathered data over C2 channels. |
Countermeasures against this campaign

- **Cyber Hygiene Matters!**
  - Check before clicking links and downloading files

- While preventing malware downloads with SIGINT is very difficult, detecting and dealing with them is relatively easy.

- Deployment of AV and continuous its alert monitoring

- Firewall implicit denial setting, and in the case of WFH, Windows Firewall setting is recommended on the host side as well.
Conclusions

- LuoYu is increasing its attack scope to companies and users in East Asia, including Japan (and their branches in China).

- Notable TTPs
  - Arsenals having capabilities to attack multiple platforms
  - Utilization of popular shared tools (i.e., ShadowPad, PlugX)
  - Various attack vector such as SIGINT, watering hole attacks, etc.

- LuoYu’s evolution throughout 2021 indicates its potential in developing into a more sophisticated group in the future
Reference

- https://www.fortinet.com/blog/threat-research/chinese-targeted-trojan-analysis
- https://blogs.jpcert.or.jp/ja/2021/10/windealer.html
- https://www.shuzhiduo.com/A/8Bz8k3Pxdx/
- https://bbs.kafan.cn/thread-2157062-1-1.html
## IoCs

<table>
<thead>
<tr>
<th>No</th>
<th>Malware Type</th>
<th>Version</th>
<th>File Name</th>
<th>MD5</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>WinDealer</td>
<td>18.19.0628</td>
<td>version.dll</td>
<td>6102f77c85541d00b4c3bc95f100fbeb</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>18.20.1225</td>
<td>qbupd.exe</td>
<td>D9A6725B6A2B38F96974518EC9E361AB</td>
</tr>
<tr>
<td>3</td>
<td></td>
<td>18.20.1225</td>
<td>NewsClientPlugin.exe</td>
<td>76ba5272a17fdab7521ea21a57d23591</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td>18.20.1225</td>
<td>RuntimeBroker.exe</td>
<td>cc7207f09a6fe41c71626ad4d3f127ce</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>C2</th>
<th>Domain/IP</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>WinDealer</td>
<td>113.62.0.0/15 111.120.0.0/14</td>
<td>Using 55556/TCP, 6999/UDP</td>
</tr>
<tr>
<td></td>
<td>221.195.68.71/32</td>
<td></td>
</tr>
<tr>
<td></td>
<td>122.112.245.55/32</td>
<td></td>
</tr>
</tbody>
</table>
THANK YOU!
Any Questions?

TEAM T5
Persistent Cyber Threat Hunters