Chinese Malware Appears in Earnest Across Cybercrime Threat Landscape

proofpoint.com/us/blog/threat-insight/chinese-malware-appears-earnest-across-cybercrime-threat-landscape

September 13, 2023

Blog

Threat Insight

Chinese Malware Appears in Earnest Across Cybercrime Threat Landscape

September 20, 2023 Proofpoint Threat Research Team

Key Takeaways

- Proofpoint has observed an increase in activity from specific malware families targeting Chinese-language speakers.
- Campaigns include Chinese-language lures and malware typically associated with Chinese cybercrime activity.
- Newly observed ValleyRAT is emerging as a new malware among Chinese-themed cybercrime activity, while Sainbox RAT and related variants are recently active as well.
- The increase in Chinese language malware activity indicates an expansion of the Chinese malware ecosystem, either through increased availability or ease of access to payloads and target lists, as well as potentially increased activity by Chinese speaking cybercrime operators.

Overview

Since early 2023, Proofpoint observed an increase in the email distribution of malware associated with suspected Chinese cybercrime activity. This includes the attempted delivery of the Sainbox Remote Access Trojan (RAT) – a variant of the commodity trojan Gh0stRAT – and the newly identified ValleyRAT malware. After years of this malware not appearing in Proofpoint threat data, its appearance in multiple campaigns over the last six months is notable.

The phrase “Chinese-themed” is used to describe any of the observed content related to this malicious activity, including lures, malware, targeting, and any metadata that contains Chinese language usage. Campaigns are generally low-volume and are typically sent to global organizations with operations in China. The email subjects and content are usually written in Chinese, and are typically related to business themes like invoices, payments, and new products. The targeted users have Chinese-language names spelled with Chinese-language characters, or specific company email addresses that appear to align with businesses' operations in China. Although most campaigns have targeted Chinese speaking users, Proofpoint observed one campaign targeting Japanese organizations, suggesting a potential expansion of activity.

These recently identified activity clusters have demonstrated flexible delivery methods, leveraging both simple and moderately complex techniques. Commonly, the emails contain URLs linking to compressed executables that are responsible for installing the malware. However, Proofpoint has also observed Sainbox RAT and ValleyRAT delivered via Excel and PDF attachments containing URLs linking to compressed executables.

Proofpoint researchers assess those multiple campaigns delivering Sainbox RAT and ValleyRAT contain some similar tactics, techniques, and procedures (TTPs). However, research into additional activity clusters utilizing these malwares demonstrate enough variety in infrastructure, sender domains, email content, targeting, and payloads that researchers currently conclude that all use of these malwares and associated campaigns are not attributable to the same cluster, but likely multiple distinct activity sets.

The emergence and uptick of both novel and older Chinese-themed malware demonstrates a new trend in the overall 2023 threat landscape. A blend of historic malware such as Sainbox – a variant of the older Gh0stRAT malware – and the newly uncovered ValleyRAT may challenge the dominance that the Russian-speaking cybercrime market has on the threat landscape. However, the Chinese-themed malware is currently mostly targeted toward users that likely speak Chinese. Proofpoint continues to monitor for evidence of increasing adoption across other languages.

For network defenders, we include several indicators of compromise and Emerging Threats detections to provide the community with the ability to cover these threats.

Campaign Details

Proofpoint has observed over 30 campaigns in 2023 leveraging malware typically associated with Chinese cybercrime activity. Nearly all lures are in Chinese, although Proofpoint has also observed messages in Japanese targeting organizations in that country.

Gh0stRAT / Sainbox

Proofpoint has observed an increase in a variant of Gh0stRAT Proofpoint researchers refer to as Sainbox. Sainbox was first identified by Proofpoint in 2020 and is referred to as FatalRAT by third-party researchers. Since April 2023, Proofpoint has identified nearly 20 campaigns delivering Sainbox after being completely absent from the email threat landscape for years.

Gh0stRAT is a RAT that was first observed in 2008. The builder for this RAT is available online. The source code is also publicly available and various modifications have been made to Gh0stRAT over the years by multiple authors and threat actors, including forked variants like Sainbox. Proofpoint has also observed a handful of Chinese language campaigns in 2023 delivering older Gh0stRAT variants.

Nearly all the observed Sainbox campaigns used invoice themed lures which spoofed Chinese office and invoicing companies. The emails were typically sent from Outlook or other freemail email addresses and contained URLs, or Excel attachments containing URLs, that linked to a zipped executable that installed Sainbox.

For example, on 17 May 2023, Proofpoint observed a campaign targeting dozens of companies, the majority of which included those in the manufacturing and technology sectors. Emails purported to be:

From: "友发票 " <lwplbh@cluedk[.]com> (Machine translation: “UF Invoice”)
With Subject: 《发票信息》(Machine translation: “Invoice Information”)

Figure 1: Email sample from 17 May 2023 delivering Sainbox.

These emails contained a URL which linked to a zipped executable, “26866498.exe”. If executed, it led to the installation of Sainbox RAT associated with the command and control (C2) “fakaka16[.]top:3366.” Proofpoint observed nearly 10 Sainbox RAT campaigns where the C2 had variations of “fakaka” in the domain, sometimes ending in a number increasing in sequential order. Additionally, “Jiangsu Bangning Science & Technology Co. Ltd” is responsible for the registration of several C2 domains associated with this actor starting with fakaka9[.]top in March 2023.

The majority of Sainbox RAT campaigns occurred between December 2022 and May 2023. Retrospective analysis of identified campaigns uncovered one more campaign in Proofpoint data using similar TTPs in April 2022. Proofpoint continues to see additional campaigns associated with this activity cluster in August 2023.

Purple Fox

The malware component of Purple Fox has been available since at least 2018. It is delivered via various methods, including historically via the Purple Fox Exploit Kit. In recent years, public reporting identified examples of Purple Fox malware delivery that was masquerading as legitimate application installers.

Proofpoint identified at least three campaigns delivering Purple Fox. While historic activity aligns with what Proofpoint considers Chinese-themed, it is rarely observed in our threat data. Notably, one observed campaign used Japanese language invoice themes targeting organizations in Japan to deliver zipped LNK attachments that led to the installation of Purple Fox, while others used Chinese language invoice themed messages with URLs leading to Purple Fox.

Proofpoint does not attribute all the Chinese-themed malware campaigns to the same threat actor at this time, but some activity clusters do overlap, suggesting threat actors may be using the same infrastructure to deliver multiple malware families.

A New Malware Joins the Fray

ValleyRAT

In March 2023, Proofpoint identified a new malware we dubbed ValleyRAT. The campaigns distributing this malware were conducted in Chinese, and, following the trend of other Chinese malware campaigns, the majority used invoice themes related to various Chinese businesses. In 2023, Proofpoint has observed at least six campaigns delivering ValleyRAT malware.

The first campaign was observed on 21 March 2023. Emails contained a URL that led to a zipped executable that downloaded the ValleyRAT payload. Subsequent campaigns contained similar TTPs including using freemail senders such as Outlook, Hotmail and WeCom to deliver URLs leading to the installation of ValleyRAT. However, in at least one campaign, the RAT was delivered via a Rust language-based loader still currently under investigation. The loader additionally downloaded a legitimate tool, EasyConnect in addition to a trojanized DLL that the tool would load and execute via DLL search order high jacking. EasyConnect is an SSL VPN appliance that enables remote access and management of Windows hosts. Subsequent campaigns in June 2023 included the same TTPs.

ValleyRAT was first publicly reported on by the Chinese cybersecurity firm Qi An Xin earlier this year.

While most of the campaigns used invoice themed lures, Proofpoint observed one outlier campaign on 24 May 2023 that used resume-themed PDFs containing URLs that, if clicked, downloaded a remote, zipped payload to install ValleyRAT.

Figure 2: PDF lure used to deliver ValleyRAT.

Analysis of the newly observed ValleyRAT indicates the possibility that one group is behind both the new malware campaigns and the resurgence of the older Purple Fox and Sainbox malware, but the timing may be coincidental rather than directly attributable.

Malware Analysis

ValleyRAT initially begins by searching for the existence of the directory "C:\Program Files\VMware\VMware Tools" on the victim machine. It then proceeds to search for specific processes within that directory: "VMwareService.exe", "VMwareTray.exe", and "VMwareUser.exe". The next step

involves a check to see if the computer is part of the "WORKGROUP" or not. It then performs a check on the total physical memory to determine if it is below the threshold of 1,173,624,064 bytes. Finally, the program checks if the size of the hard disk drive (HDD) is below 110GB, these checks are basic virtualization or emulation checks to attempt to identify if the payload is being executed within in a virtual environment.

ValleyRAT is a RAT written in C++, compiled in Chinese and demonstrates the functionalities of a typically basic RAT. The following table is an overview of the commands that are currently implemented in what Proofpoint assess is version 3.0 of ValleyRAT, an assessment derived from a “version” number that returns a 3.0 string value. When the system information packet is sent, the C2 replies with command packets. It currently has the following commands implemented:

Command	Description
0x00	Plugin cleanup, and get system's process list. Client replies with a STRUCT_PACKET_PROCESS_LIST structure.
0x01	Reply with STRUCT_PACKET_0x02 structure, that contains the exact data originally sent to the Client. This is probably implemented as anti-bot verification or as a PING→PONG packet.
0x02	Drops and executes a DLL
0x04	Drops and executes a DLL (Second Method)
0x05	Plugin cleanup, replays with a STRUCT_PACKET_0x05 structure.
0x06	Get system's process list. Client replies with a STRUCT_PACKET_PROCESS_LIST structure.
0x07	Drops and executes any type of file (document, image, etc)
0x08	Downloads and executes an executable file.
0x09	Sets the Client to start at system startup.
0x0A	Sets the "BEIZHU" ("remark") or "FENZU" ("subgroup") registry keys.
0x64	Stops the client, without terminating the process.
0x65	Starts the client

Table 1: ValleyRAT commands and associated descriptions.

Packet Process List

STRUCT_PACKET_PROCESS_LIST

```
struct STRUCT_PACKET_PROCESS_LIST {
    byte        code;           // set to 0x02
    byte        reserved;       // not used, set to 0x00
    wchar_t     data[0x3A98];   // client name, PID, module name, thread id and window name, followed by "--" separated of process names
};
```

Figure 3: Structure which defines the content of a packet sent to the C2 to describe running processes, window names, etc.

STRUCT_PACKET_0x02

```
struct STRUCT_PACKET_0x02 {
    byte    code;           // set to 0x05
    byte    data[0x20470];  // original data sent by the C2
};
```

STRUCT_PACKET_0x05

```
struct  STRUCT_PACKET_0x05 {
    byte       code;            // set to 0x05
    byte        reserved;       // not used, set to 0x00
    wchar_t     data[0xFF];     // "插件清理完成", roughly translated to "Plugin cleanup complete"
};
```

Figure 4: Structure which defines the content of a packet sent to the C2 to indicate a plugin has been cleaned up.

Communication Protocol

The malware uses raw sockets with a custom protocol to communicate with the C2 (see Figure 7 for packet encoding). Before receiving any commands from the Server, the Client announces itself by sending a packet containing system information, formatted in the following structure:

STRUCT_PACKET_SYSINFO

```
struct STRUCT_PACKET_SYSINFO {
    byte        code;                           // set to 0x03
    byte        reserved;                       // set to 0x00, not used
    wchar_t     szw_ip_info[255];               // system IP addresses
    wchar_t     status[10];                     // client status, can be either "闲" (idle) or "忙" busy
    wchar_t     szw_os_info[100];               // computer name and windows version
    wchar_t     szw_kernel_info[30];            // ntdll.dll version
    wchar_t     szw_cpu_info[60];               // CPU information
    wchar_t     szw_hdd_info[200];              // HDD and storage devices information
    wchar_t     szw_gpu_info[60];               // GPU information
    wchar_t     szw_foreground_window_name[255];// name of the topmost window
    wchar_t     szw_subgroup[50];               // comes from the "FENZU" ("subgroup") reg key and is set to "默认" ("default")
    wchar_t     szw_remark[50];                 // comes from the "BEIZHU" ("remark") reg key and is set to "2023. 5"
    wchar_t     szw_exec_time[50];              // time last command execution took
    wchar_t     szw_uptime[50];                 // current time and total uptime
    wchar_t     szw_arch[5];                    // RAT architecture, in this case X86
    wchar_t     szw_pid[30];                    // RAT process ID
    wchar_t     szw_cpu_arch[30];               // system architecture
    wchar_t     szw_username[50];               // system username
    wchar_t     szw_admin_rights[5];            // user admin rights, can be either "有" ("have") or "无" ("none")
    wchar_t     szw_has_camera[10];             // camera access, can be either "有" ("have") or "无" ("none")
    wchar_t     szw_qq_info[255];               // get QQ ID and plugins
    wchar_t     szw_antivirus_info[50];         // get installed antivirus
    wchar_t     szw_system_language[32];        // get system's language
    wchar_t     szw_monitor_info[255];          // get system's monitors information
    wchar_t     szw_system_directory[50];       // system directory
    wchar_t     szw_system_id[49];              // system id, check Appendix for generation algorithm
};
```

Figure 5: Structure which defines the content of the initial system information beacon that it sends to the C2 to identify a newly infected victim.

Packet Decoding Algorithm

```python
import zlib
import struct

def get_wchar(data):
    result = b""
    for i in range(0, len(data), 2):
        b = data[i:i+2]
        if b == b"\x00\x00":
            break
        result += b
    return result

def dump(data):
    for i, b in enumerate(data):
        print("%02X " % b, end="")
        if (i+1)%0x10 == 0:
            print()
    print()

def decode_packet(data):
    o = 0

    size, size_b = struct.unpack_from("<LL", data, o)
    o += 4
    if size == size_b:
        o += 4

    c_id = get_wchar(data[o:])
    o += len(c_id) + 2

    size_raw, = struct.unpack_from("<L", data, o)
    o += 4

    packet_data = zlib.decompress(data[o:o+size])

    print(c_id.decode("utf-16le"))
    if len(packet_data) <= 0x100:
        dump(packet_data)
    else:
        open("packet_out.bin", "wb").write(packet_data)

filename = "sysinfo.pck.bin"
decode_packet(open(filename, "rb").read())
```

Figure 6: Network Decoding Algorithm.

SystemID Generation Algorithm

ValleyRAT generates an MD5 digest of the following values: OS Info, Kernel Version, CPU Name, Architecture, IsAdmin, Hardware Profile GUID to use as a System Identifier (SystemID). Below is a reimplementation of this in Python.

system id generation algorithm

```python
import hashlib

def generate_system_id():
    data = b""   # STRUCT_PACKET_SYSINFO.szw_os_info
    data += b""  # STRUCT_PACKET_SYSINFO.szw_kernel_version
    data += b""  # STRUCT_PACKET_SYSINFO.szw_cpu_name
    data += b""  # STRUCT_PACKET_SYSINFO.szw_client_arch "X86"
    data += b""  # STRUCT_PACKET_SYSINFO.szw_admin_rights "有" or "无"
    data += b""  # HW_PROFILE_INFOW.szHwProfileGuid

    return hashlib.md5(data).hexdigest()
```

Figure 7: SystemID generation.

Conclusion

For over a decade, Gh0stRAT and related variants have been consistently exploited in various circles. Proofpoint recently observed a minor resurgence in the use of Sainbox and other Chinese-themed malware, piquing the interest of analysts who can assess the broader impact of older malware. With this resurgence, the questions arise: is the impact of older malware easier to detect due to its age? Does mature detection always mean mature security? Based on Proofpoint's analysis, the answer is not necessarily, as older malware can still be effective, especially when threat actors constantly change tactics by rotating IPs, domains, encoding, and obfuscation. Consequently, even though these malware families are not new, organizations cannot afford to underestimate the risk they pose.

Proofpoint research suggests that this activity does not seem to be related to a single entity but rather appears to be a cluster of activities based on temporal patterns. The appearance of ValleyRAT alongside the older families hints at the possibility of their relation in terms of timing. Proofpoint anticipates ValleyRAT will be used more frequently in the future.

Raising awareness in 2023 about the reappearance of these threats serves as an informational bulletin for the community. While new and sophisticated threats seemingly dominate the daily threat landscape, it is essential to maintain a balanced perspective by acknowledging seemingly less significant risks that persist. Despite being neither new nor advanced, Sainbox RAT still poses a threat in 2023, and ValleyRAT is an emerging threat in this space.

Emerging Threats Signatures

- 2045774 - ET INFO Observed URL Shortening Service Domain in DNS Lookup (dwz .mk)
- 2045775 - ET INFO Observed URL Shortening Service Domain (dwz .mk in TLS SNI)
- 2854367 - ETPRO MALWARE Win32/ValleyRat CnC Activity (GET) M1
- 2854368 - ETPRO MALWARE Win32/ValleyRat CnC Activity (GET) M2
- 2854369 - ETPRO MALWARE Win32/ValleyRat CnC Activity via tcp Outbound
- 2854370 - ETPRO MALWARE Win32/ValleyRat CnC Activity via tcp Inbound
- 2854371 - Suspicious User-Agent in HTTP Request (GameInfo)
- 2044739 - ET INFO Chinese CDN Domain in DNS Lookup (ctcontents .com) (info.rules)

Example IOCs

Indicator	Description	First Observed
hxxp://rus3rcqtp[.]hn-bkt[.]clouddn[.]com/26866498[.]zip	Sainbox Payload URL	May-23
0d133dde99d883274bf5644bd9e59af3c54c2b3c65f3d1bc762f2d3725f80582	Sainbox Executable SHA256	May-23
fakaka16[.]top:3366	Sainbox C2	May-23
lwplbh@cluedk[.]com	Sainbox Sender Email	May-23
7f32ca98ce66a057ae226ec78638db95feebc59295d3afffdbf407df12b5bc79	Sainbox Executable SHA256	Aug-23
kakafa[.]top:3367	Sainbox C2	Aug-23
q1045582630@qq[.]com	Sainbox Sender Email	Aug-23
hxxp://51fapiaoyun[.]com/%E5%8F%91-%E7%A5%A8[.]rar	ValleyRAT Payload URL	Mar-23
http://124[.]220[.]35[.]63/laoxiang[.]exe	ValleyRAT Payload URL	Mar-23
cjkmj@51fapiao[.]com	ValleyRAT Sender Email	Mar-23
a48abe2847e891cfd6c18c7cdaaa8e983051bc2f7a0bd9ef5c515a72954e1715	PDF Used to Deliver ValleyRAT SHA256	May-23
a48abe2847e891cfd6c18c7cdaaa8e983051bc2f7a0bd9ef5c515a72954e1715	ValleyRAT Executable	May-23

C:\Users\77\source\repos\Project8\Debug\Project8.pdb	ValleyRAT PDB File Path	May-23
hxxps://drfs[.]ctcontents[.]com/file/40788929/860577489/0823d7/%E4%B8%AA%E4%BA%BA%E7%AE%80%E5%8E%862023[.]rar	ValleyRAT Payload URL	May-23
aa0035@zohomail[.]cn	ValleyRAT Sender Email	May-23
hxxp://ckj2[.]cn/R8F	ValleyRAT Payload URL	May-23
4f01ffe98009a8090ea8a086d21c62c24219b21938ea3ec7da8072f8c4dcc7a6	ValleyRAT Executable	May-23
vip66@xqxayjrk101[.]wecom[.]work	ValleyRAT Sender Email	May-23
hxxps://zc1800[.]oss-cn-shenzhen[.]aliyuncs[.]com/piao	ValleyRAT Payload URL	Jun-23
qdjvqvumsdw@hotmail[.]com	ValleyRAT Sender Email	Jun-23
hxxps://fhyhdf[.]oss-cn-hangzhou[.]aliyuncs[.]com/%E7%99%BC%E7%A5%A8[.]zip	ValleyRAT Payload URL	Jun-23
kweffabibis0@outlook[.]com	ValleyRAT Sender Email	Jun-23