WinDealer dealing on the side

By GReAT

Published: 2022-06-02 · Archived: 2026-04-05 21:52:51 UTC

Introduction

LuoYu is a lesser-known threat actor that has been active since 2008. It primarily goes after targets located in China, such as foreign diplomatic organizations established in the country, members of the academic community, or companies from the defense, logistics and telecommunications sectors. In their initial disclosures on this threat actor, TeamT5 identified three malware families: SpyDealer, Demsty and WinDealer. The actor behind these families is capable of targeting Windows, Linux and macOS machines, as well as Android devices.

In previous years, Kaspersky investigated LuoYu's activities and was able to confirm the connection between Demsty and WinDealer. On January 27, we delivered a joint presentation with TeamT5 and ITOCHU Corporation at Japan Security Analyst Conference (JSAC) to provide an update on the actor's latest activities. In this article, we will focus on one of the most groundbreaking developments: the fact that LuoYu has the ability to perform man-on-the-side attacks.

Delivery method

In the past, LuoYu used watering-hole attacks (for instance, on local news websites) to infect their targets. Seeing that some variants of their Android malware impersonate a popular messaging app in Asia, it is also likely that malicious APKs are distributed in a variety of ways, including social engineering to convince users to install fake updates for their applications.

In 2020, we discovered a whole new distribution method for the WinDealer malware that leverages the automatic update mechanism of select legitimate applications. In one case we investigated, we noticed that a signed executable qgametool.exe (MD5 f756083b62ba45dcc6a4d2d2727780e4), compiled in 2012, deployed WinDealer on a target machine. This program contains a hardcoded URL that it uses to check for updates, as shown in the following screenshot:

```
.text:00402D16 loc_402D16:                             ; CODE XREF: WinMain(x,x,x,x)+162↑j
.text:00402D16                                         ; WinMain(x,x,x,x)+1A2↑j
.text:00402D16                 mov     [ebp+String1], offset download_src ; "http://download.pplive.com/PPTV(pplive)"...
.text:00402D1D                 mov     eax, [ebp+String1] ; http://download.pplive.com/PPTV(pplive)_forap_1084_9993.exe
.text:00402D20                 push    eax
.text:00402D21                 push    offset aLoaderPszurlS ; "[Loader] pszUrl:%s"
.text:00402D26                 push    offset unk_4091C8 ; this
.text:00402D2B                 call    ?Format@CString@@QAAXPBDZZ ; CString::Format(char const *,...)
```

Update URL hardcoded in qgametool.exe

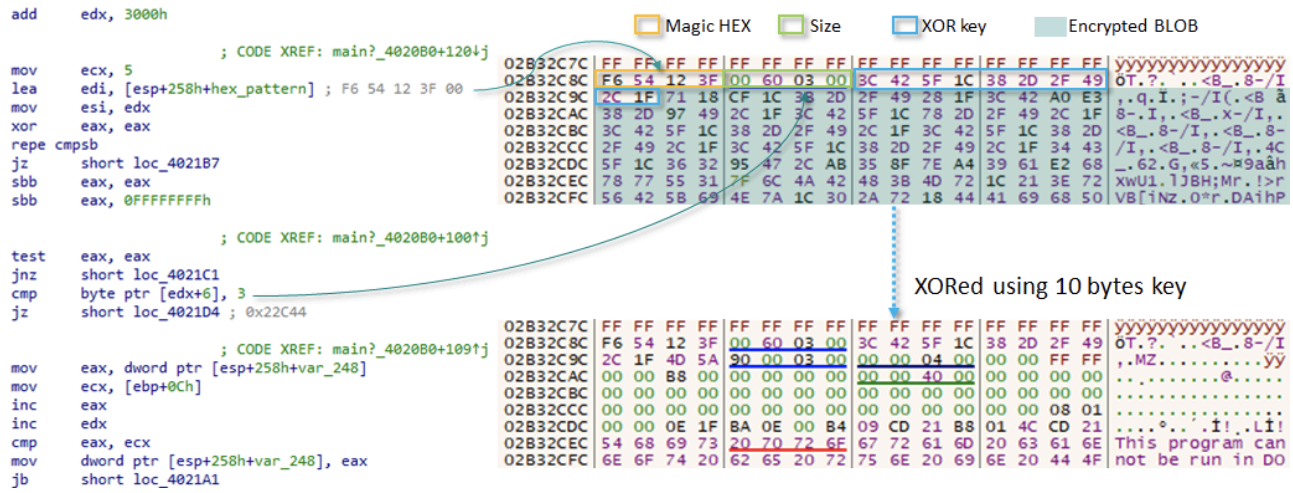
The executable located at this URL (hxxp://download.pplive[.]com/PPTV(pplive)_forap_1084_9993.exe, MD5 270902c6bb6844dc25ffaec801393245) is benign, but our telemetry shows that on rare occasions, a WinDealer sample (MD5 ce65092fe9959cc0ee5a8408987e3cd4) is delivered instead.

Observed WinDealer infection flow

We also identified online message board posts where Chinese-speaking users reported the discovery of malware under the same name – PPTV(pplive)_forap_1084_9993.exe – on their machine. The posted information was complete enough for us to confirm that they had indeed received a sample of WinDealer.
Leaving the mystery of the delivery method aside for now, let's look at the capabilities of the malware itself.

WinDealer's technical description

WinDealer is a modular malware platform. It starts execution by locating an embedded DLL file placed in its resources by looking for a hardcoded pattern, and proceeds to decode it using a 10-byte XOR key.



Layout of the encrypted data

WinDealer's logic is spread over the initial EXE and its companion DLL: the former contains the setup of the program as well as network communications, while the orders sent by the C2 are implemented in the latter. The malware possesses the following capabilities:

- File and file system manipulation: reading, writing and deleting files, listing directories, obtaining disk information;

- Information gathering: collecting hardware details, network configuration and/or keyboard layout, listing running processes, installed applications and configuration files of popular messaging applications (Skype, QQ, WeChat and Wangwang);
- Download and upload of arbitrary files;
- Arbitrary command execution;
- System-wide search across text files and Microsoft Word documents;
- Screenshot capture;
- Network discovery via ping scan;
- Backdoor maintenance: set up or remove persistence (via the registry's RUN key), configuration updates.

A variant we discovered (MD5 26064e65a7e6ce620b0ff7b4951cf340) also featured the ability to list available Wi-Fi networks. Overall, WinDealer is able to collect an impressive amount of information, even when compared to other malware families. And yet, the most extraordinary aspect of WinDealer lies elsewhere.

The impossible infrastructure

The latest WinDealer sample we discovered in 2020 doesn't contain a hardcoded C2 server but instead relies on a complex IP generation algorithm to determine which machine to contact. The details of this algorithm are left as an exercise to the reader, but the end result is that the IP address is selected **at random** from one of these two ranges:

- 113.62.0.0/15 (AS4134, CHINANET XIZANG PROVINCE NETWORK)
- 111.120.0.0/14 (AS4134, CHINANET GUIZHOU PROVINCE NETWORK)

Once the IP address has been selected, communications take place either over UDP port 6999 or TCP port 55556. In an even weirder twist, a research partner shared with us an additional WinDealer sample (MD5 d9a6725b6a2b38f96974518ec9e361ab) that communicates with the hardcoded URL "http://www[.]microsoftcom/status/getsign.asp". This domain is obviously invalid and cannot resolve to anything in normal circumstances – yet the malware expects a response in a predetermined format ("\x11\x22\x?? \x33\x44").

Packets exchanged with the C2 server contain a header (described in the next table) followed by AES-encrypted data. They leverage a homemade binary protocol containing magic numbers and flags, making it easy to recognize and filter packets on a large scale.

Offset	Description	Sample value (in hex)
0x00	Magic number	06 81 DA 91 CE C7 9F 43
0x08	Target identifier	57 5B 73 B2
0x0C	Flag set by the attacker. Its exact meaning remains unclear	00 or 0B or 16

0x0D	Connection type or backdoor command identifier 0 = initial connection 1 = subsequent connection Others = backdoor command identifiers	00
0x0E	Unknown static value	14
0x0F	Unknown value	00
0x10	Payload Initial connection: the generated AES key and its CRC32, encrypted using RSA-2048 with a hardcoded public key. All other packets: payload size followed by encrypted payload using AES-128 in ECB mode with the generated AES key.	03 4D 5D 44 C3 1E 0A DA A3 4A 86 A3 CC ED 67 38 …

The man-on-the-side attack

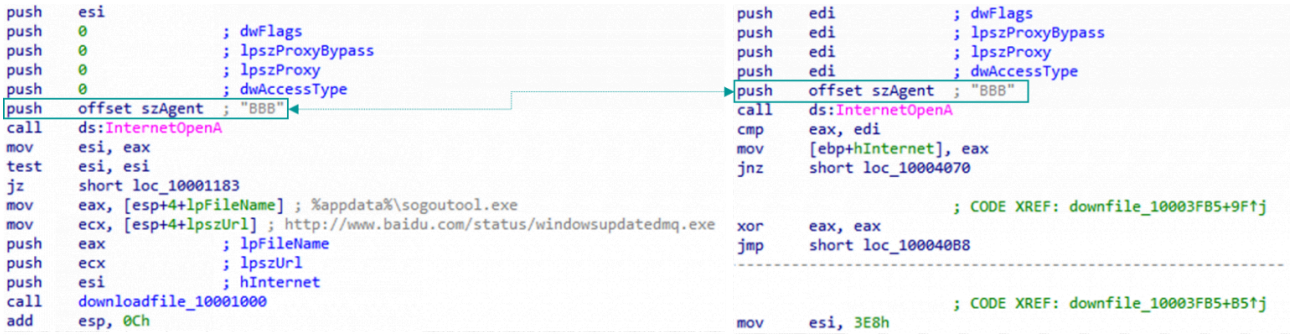
Putting all the pieces together, WinDealer's infrastructure is nothing short of extraordinary:

- It appears to be distributed via plain HTTP requests that normally return legitimate executables.
- It communicates with IP addresses selected randomly inside a specific AS.
- It can interact with non-existent domain names.

It is very hard to believe that an attacker would be able to control the 48,000 IP addresses of the aforementioned IP ranges, or even a significant portion of them. The only way to explain these seemingly impossible network behaviors is by assuming the existence of a man-on-the-side attacker who is able to intercept all network traffic and even modify it if needed.

Such capabilities are not unheard of: the QUANTUM program revealed in 2014 was the first known instance. The general idea is that when the attacker sees a request for a specific resource on the network, it tries to reply to the target faster than the legitimate server. If the attacker wins the "race", the target machine will use the attacker-supplied data instead of the normal data. This is consistent with the scenario described earlier in this article, where the target receives an infected executable instead of the normal one. Automatic updaters are prime targets for such attacks as they perform frequent requests – it doesn't matter if the attackers don't win most races, as they can try again until they succeed, guaranteeing that they will infect their targets eventually. This class of attack is particularly devastating because there is nothing users can do to protect themselves, apart from routing traffic through another network. This can be done with the use of a VPN, but these may be illegal depending on the jurisdiction and would typically not be available to Chinese-speaking targets.

Confirming our assessment, we later discovered a downloader utility (MD5 4e07a477039b37790f7a8e976024eb66) that uses the same unique user-agent as WinDealer samples we analyzed ("BBB"), tying it weakly to LuoYu.



A downloader utility and WinDealer of 2021 use the unique user-agent "BBB"

The downloader periodically retrieves and runs an executable from hxxp://www.baidu[.]com/status/windowsupdatedmq.exe. This URL normally returns a 404 error and we consider it extremely unlikely that the attackers have control over this domain.

Based on all the evidence laid out above, we speculate that the attackers may have the following capabilities over AS4134:

- Intercepting all network traffic, which allows them to receive backdoor responses to random IP addresses without having to deploy actual C2 servers.
- Injecting arbitrary TCP and UDP packets on the network, a capability through which they can send orders to WinDealer.
- Full control over the DNS, meaning they can provide responses for non-existent domains.
- Either QUANTUMINSERT capabilities or the ability to modify the contents of HTTP packets on the fly, thanks to which they can achieve remote, zero-click malware installation by abusing auto-update mechanisms. One noteworthy observation is that the attackers specifically target plain HTTP sessions, indicating that they may not have the ability to break or downgrade HTTPS.

WinDealer's targets

Our analysis of WinDealer reveals that it specifically looks for popular applications in Asia, such as QQ, WeChat and WangWang. It also contains references to registry keys created by Sogou programs. This indicates to us that the LuoYu APT is predominantly focused on Chinese-speaking targets and organizations related to China. Our telemetry confirms that the vast majority of LuoYu targets are located in China, with occasional infections in other countries such as Germany, Austria, the United States, Czech Republic, Russia and India.

In recent months, LuoYu has started to widen its scope to companies and users in East Asia and their branches located in China.

Geographic distribution of WinDealer targets

Conclusion

With this report, we recognize LuoYu as an extremely sophisticated threat actor able to leverage capabilities available only to the most mature attackers. We can only speculate as to how they were able to obtain such capabilities. They could have compromised routers on the route to (or inside) AS4134. Alternatively, they may use signals intelligence methods unknown to the general public. They may even have access (legitimate or fraudulent) to law enforcement tools set up at the ISP level and are abusing them to perform offensive operations. Overall, a threat actor is leveraging capabilities that could be compared (but are distinct) from the QUANTUMINSERT program in order to infect targets located in China.

Man-on-the-side attacks are devastating because they do not require any interaction with the target to lead to a successful infection: simply having a machine connected to the internet is enough. They can only be detected through careful network monitoring, which is outside of the realm of everyday users, or if an endpoint security program catches the payload when it is deployed on the attacked computer.

Whatever the case, the only way for potential targets to defend against such intrusions is to remain extremely vigilant and have robust security procedures involving regular antivirus scans, analysis of outbound network traffic and extensive logging to detect anomalies.

Indicators of Compromise

WinDealer samples

MD5: ce65092fe9959cc0ee5a8408987e3cd4
SHA-1: 87635d7632568c98c0091d4a53680fd920096327
SHA-256: 27c51026b89c124a002589c24cd99a0c116afd73c4dc37f013791f757ced7b7e

MD5: 0c8663bf912ef4d69a1473597925feeb
SHA-1: 78294dfc4874b54c870b8daf7c43cfb5d8c211d0
SHA-256: db034aeb3c72b75d955c02458ba2991c99033ada444ebed4e2a1ed4c9326c400

MD5: 1bd4911ea9eba86f7745f2c1a45bc01b
SHA-1: f64c63f6e17f082ea254f0e56a69b389e35857fd
SHA-256: 25cbfb26265889754ccc5598bf5f21885e50792ca0686e3ff3029b7dc4452f4d

MD5: 5a7a90ceb6e7137c753d8de226fc7947
SHA-1: 204a603c409e559b65c35208200a169a232da94c
SHA-256: 1e9fc7f32bd5522dd0222932eb9f1d8bd0a2e132c7b46cfcc622ad97831e6128

MD5: 73695fc3868f541995b3d1cc4dfc1350
SHA-1: 158c7382c88e10ab0208c9a3c72d5f579b614947
SHA-256: ea4561607c00687ea82b3365de26959f1adb98b6a9ba64fa6d47a6c19f22daa4

MD5: 76ba5272a17fdab7521ea21a57d23591
SHA-1: 6b831413932a394bd9fb25e2bbdc06533821378c
SHA-256: ecd001aeb6bcbafb3e2fda74d76eea3c0ddad4e6e7ff1f43cd7709d4b4580261

MD5: 8410893f1f88c5d9ab327bc139ff295d
SHA-1: 64a1785683858d8b6f4e7e2b2fac213fb752bae0
SHA-256: 318c431c56252f9421c755c281db7bd99dc1efa28c44a8d6db4708289725c318

MD5: cc7207f09a6fe41c71626ad4d3f127ce
SHA-1: 84e749c37978f9387e16fab29c7b1b291be93a63
SHA-256: 28df5c75a2f78120ff96d4a72a3c23cee97c9b46c96410cf591af38cb4aed0fa

MD5: e01b393e8897ed116ba9e0e87a4b1da1
SHA-1: 313b231491408bd107cecf0207868336f26d79ba
SHA-256: 4a9b37ca2f90bfa90b0b8db8cc80fe01d154ba88e3bc25b00a7f8ff6c509a76f

MD5: ef25d934d12684b371a17c76daf3662c
SHA-1: b062773bdd9f8433cbd6e7642226221972ecd4e1
SHA-256: 08530e8280a93b8a1d51c20647e6be73795ef161e3b16e22e5e23d88ead4e226

MD5: faa8eaed63c4e9f212ef81e2365dd9e8
SHA-1: 0d3a5725b6f740929b51f9a8611b4f843e2e07b1
SHA-256: b9f526eea625eec1ddab25a0fc9bd847f37c9189750499c446471b7a52204d5a

---