Evasive Panda APT group delivers malware via updates for popular Chinese software

welivesecurity.com/2023/04/26/evasive-panda-apt-group-malware-updates-popular-chinese-software/

April 26, 2023

ESET Research uncovers a campaign by the APT group known as Evasive Panda targeting an international NGO in China with malware delivered through updates of popular Chinese software

Facundo Muñoz

26 Apr 2023 - 11:30AM

ESET Research uncovers a campaign by the APT group known as Evasive Panda targeting an international NGO in China with malware delivered through updates of popular Chinese software

ESET researchers have discovered a campaign that we attribute to the APT group known as Evasive Panda, where update channels of legitimate applications were mysteriously hijacked to deliver the installer for the MgBot malware, Evasive Panda's flagship backdoor.

Key points of the report:

- Users in mainland China were targeted with malware delivered through updates for software developed by Chinese companies.
- We analyze the competing hypotheses of how the malware could have been delivered to targeted users.
- With high confidence we attribute this activity to the Evasive Panda APT group.
- We provide an overview of Evasive Panda's signature backdoor MgBot and its toolkit of plugin modules.

Evasive Panda profile

Evasive Panda (also known as BRONZE HIGHLAND and Daggerfly) is a Chinese-speaking APT group, active since at least 2012. ESET Research has observed the group conducting cyberespionage against individuals in mainland China, Hong Kong, Macao, and Nigeria. Government entities were targeted in China, Macao, and Southeast and East Asian countries, specifically Myanmar, the Philippines, Taiwan, and Vietnam, while other organizations in China and Hong Kong were also targeted. According to public reports, the group has also targeted unknown entities in Hong Kong, India, and Malaysia.

The group implements its own custom malware framework with a modular architecture that allows its backdoor, known as MgBot, to receive modules to spy on its victims and enhance its capabilities.

Campaign overview

In January 2022, we discovered that while performing updates, a legitimate Chinese application had received an installer for the Evasive Panda MgBot backdoor. During our investigation, we discovered that the malicious activity went back to 2020.

Chinese users were the focus of this malicious activity, which ESET telemetry shows starting in 2020 and continuing throughout 2021. The targeted users were located in the Gansu, Guangdong, and Jiangsu provinces, as shown in Figure 1.

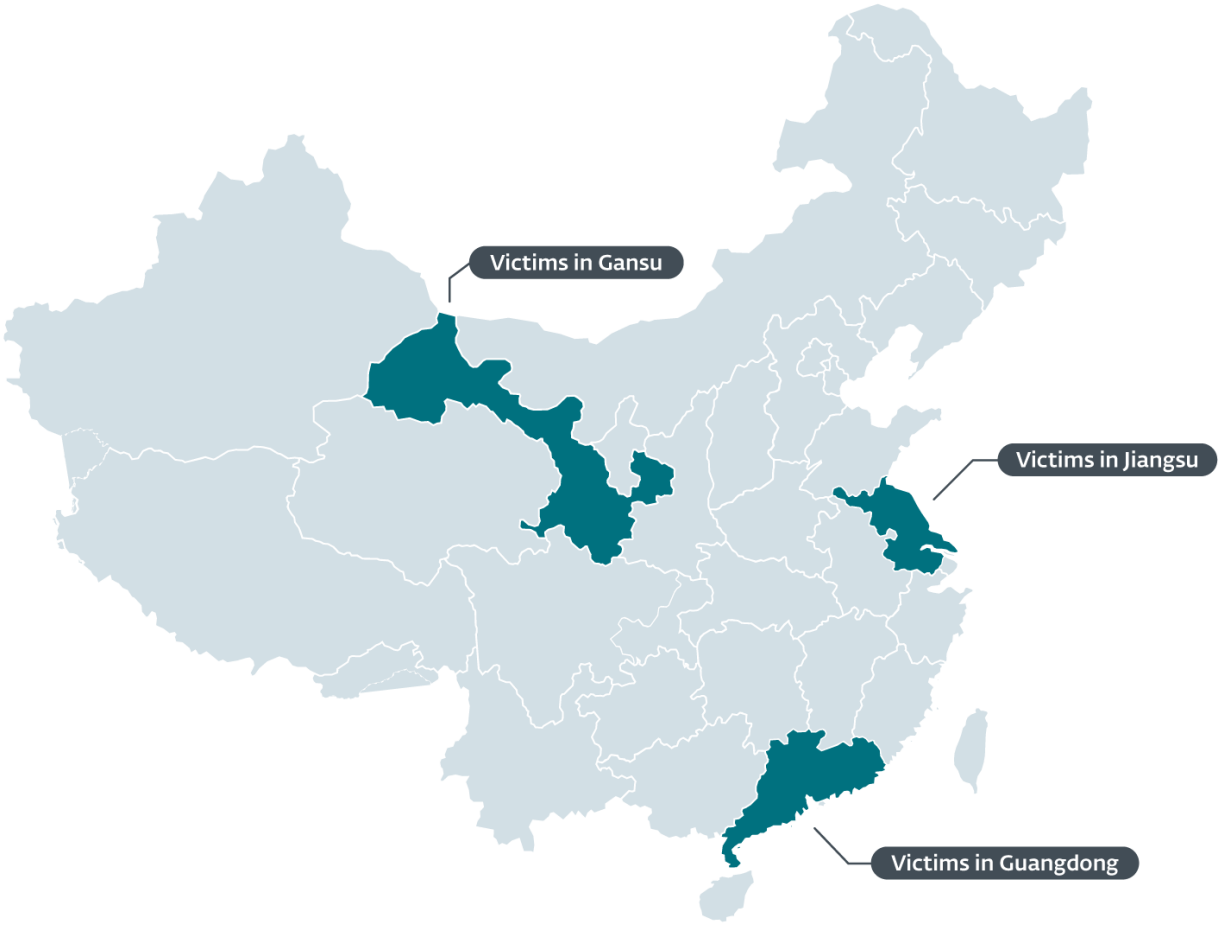

Figure 1. Map of China showing where users were targeted

The majority of the Chinese victims are members of an international NGO that operates in two of the previously mentioned provinces.

One additional victim was also discovered to be located in the country of Nigeria.

Attribution

Evasive Panda uses a custom backdoor known as MgBot, which was publicly documented in 2014 and has seen little evolution since then; to the best of our knowledge, the backdoor has not been used by any other group. In this cluster of malicious activity, only the MgBot malware was observed deployed on victimized machines, along with its toolkit of plugins. Therefore, with high confidence we attribute this activity to Evasive Panda.

Technical analysis

During our investigation, we discovered that when performing automated updates, a legitimate application software component downloaded MgBot backdoor installers from legitimate URLs and IP addresses.

In Table 1, we provide the URL from where the download originated, according to ESET telemetry data, including the IP addresses of the servers, as resolved at the time by the user's system; therefore, we believe that these IP addresses are legitimate. According to passive DNS records, all of these IP addresses match the observed domains, therefore we believe that these IP addresses are legitimate.

Table 1. Malicious download locations according to ESET telemetry

URL	First seen	Domain IP	ASN	Downloader
http://update.browser.qq[.]com/qmbs/QQ/QQUrlMgr_QQ88_4296.exe	2020-11-02	123.151.72[.]74	AS58542	QQUrlMgr.exe QQ.exe QQLive.exe QQCall<XX>.exe
183.232.96[.]107			AS56040	

URL	First seen	Domain IP	ASN	Downloader
61.129.7[.]35	AS4811			

Hypotheses of compromise

When we analyzed the likelihood of several methods that could explain how the attackers managed to deliver malware through legitimate updates, we were left with two scenarios: supply-chain compromise, and adversary-in-the-middle attacks. For both scenarios we will also take into account antecedents of similar attacks by other Chinese-speaking APT groups.

Tencent QQ is a popular Chinese chat and social media service. In the next sections, we will use the Tencent QQ Windows client software updater, QQUrlMgr.exe (listed in Table 1), for our examples, given that we have the highest number of detections from downloads by this particular component.

Supply-chain compromise scenario

Given the targeted nature of the attacks, we speculate that attackers would have needed to compromise the QQ update servers to introduce a mechanism to identify the targeted users to deliver them the malware, filtering out non-targeted users and delivering them legitimate updates – we registered cases where legitimate updates were downloaded through the same abused protocols.

While not an Evasive Panda case, a prime example of this type of compromise is in our report Operation NightScout: Supply-chain attack targets online gaming in Asia, where attackers compromised the update servers of a software developer company based in Hong Kong. According to our telemetry, more than 100,000 users had the BigNox software installed, but only five had malware delivered through an update. We suspect that the attackers compromised the BigNox API on the update server to reply to the updater component on the machines of targeted users with a URL to a server where the attackers hosted their malware; non-targeted users were sent the legitimate update URL.

Based on that antecedent, in Figure 2 we illustrate how the supply-chain compromise scenario could have unfolded according to observations in our telemetry. Still, we must warn the reader that this is purely speculation and based on our static analysis, with very limited information, of QQUrlMgr.exe (SHA-1: DE4CD63FD7B1576E65E79D1D10839D676ED20C2B).

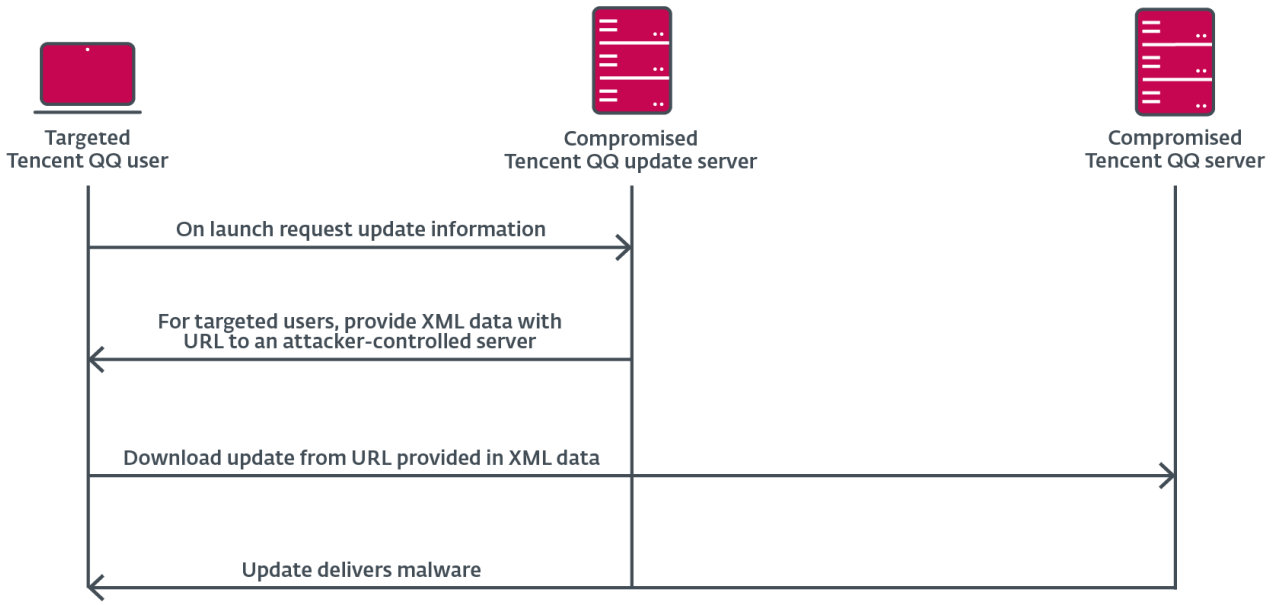

Figure 2. Sequence diagram of the hypothesized supply-chain compromise

It is also worth noting that during our research we were never able to retrieve a sample of the XML “update” data – neither a legitimate, nor a malicious, XML sample – from the server contacted by QQUrlMgr.exe. The “update check” URL is hardcoded, in obfuscated form, in the executable, as shown in Figure 3.

```
UPDATE_SERVER_URL:                      ; DATA XREF: GetUpdateInstructionsFromServer+86↑o
                text "UTF-16LE", 'hssn://i.tw.qo.ipg/eitj-bjz/rbsxgf?rukju=40&kbnnlyj'
                text "UTF-16LE", 'u=%d0655&tuju=TQEwTX7dN5Auydj9Z0X3MT3SBVtm54J1yU+an'
                text "UTF-16LE", 's9/tjxdExzhmP3y46xhEuslcsfp&ug=0',0
```

Figure 3. Obfuscated URL in the legitimate QQUrlMgr.exe binary

Deobfuscated, the complete update check URL is:

http://c.gj.qq[.]com/fcgi-bin/busxml?
busid=20&supplyid=30088&guid=CQEjCF9zN8Zdyzj5S6F1MC1RGUtw82B7yL+hpt9/gixzExnawV3y20xaEdtektfo&dm=0

The server responds with XML-formatted data encoded with base64 and encrypted with an implementation of the TEA algorithm using a 128-bit key. This data contains instructions to download and execute a file, along with other information. Since the decryption key is also hardcoded, as shown in Figure 4, it could be known to the attackers.

```
; int XML_DECRYPTION_KEY[4]
XML_DECRYPTION_KEY db '3+&7k!I~F,@#y$^d',0
```

Figure 4. Hardcoded key in the legitimate QQUrlMgr.exe binary

QQUrlMgr.exe then downloads the indicated file, unencrypted, via HTTP and hashes its contents with the MD5 algorithm. The result is checked against a hash present in the update check response XML data, as seen in Figure 5. If the hashes match, QQUrlMgr.exe executes the downloaded file. This reinforces our hypothesis that the attackers would need to control the XML server-side mechanism in the update server to be able to provide the correct MD5 hash of the malware installer.

```
QQ_PrepareDownloadPath(pParametersStructure, &pDownloadedFilePath);
...
if ( !QQ_DownloadFile(pParametersStructure->param_downloadfile_url, pDownloadedFilePath, 0) )
{
        ...
LABEL_13:
        return 0;
}

pMD5Hash = QQ_GetMD5Hash(pDownloadedFilePath);
iCmpResult = do_wcscmp(&pParametersStructure->downloadfile_md5, pMD5Hash);
...
if ( !iCmpResult )
{
        DeleteFileW(pDownloadedFilePath);
        QQ_ReportFunc(1004);
        ...
        goto LABEL_13;
}
CopyStringFromSrcToDst(&pDownloadedFilePath, &pParametersStructure->pszModuleFilePath);
```

Figure 5. QQUrlMgr.exe code that orchestrates the download of the update

We believe that this scenario would explain our observations; however, many questions are left unanswered. We reached out to Tencent's Security Response Center to confirm the legitimacy of the full URL from where the malware was downloaded; update.browser.qq[.]com is – at the time of writing – unreachable, but Tencent could not confirm whether the full URL was legitimate.

Adversary-in-the-middle scenario

On 2022-06-02, Kaspersky published a research report about the capabilities of the Chinese-speaking LuoYu APT group and their WinDealer malware. Similar to what we observed on this cluster of Evasive Panda victims, their researchers found that, since 2020, victims of LuoYu had received the WinDealer malware through updates via the legitimate application qgametool.exe from the PPTV software, also developed by a Chinese company.

WinDealer has a puzzling capability: instead of carrying a list of established C&C servers to contact in case of a successful compromise, it generates random IP addresses in the 13.62.0.0/15 and 111.120.0.0/14 ranges from China Telecom AS4134. Although a small coincidence, we noticed that the IP addresses of the targeted Chinese users at the time of receiving the MgBot malware were on the AS4134 and AS4135 IP addresses ranges.

Possible explanations for what enables these capabilities for its C&C infrastructure are that LuoYu either control a large amount of devices associated with the IP addresses on those ranges, or that they are able to do adversary-in-the-middle (AitM) or attacker-on-the-side interception on the infrastructure of that particular AS.

AitM styles of interception would be possible if the attackers – either LuoYu or Evasive Panda – were able to compromise vulnerable devices such as routers or gateways. As an antecedent, in 2019 ESET researchers discovered that the Chinese APT group known as BlackTech was performing AitM attacks through compromised ASUS routers and delivering the Plead malware through ASUS WebStorage software updates.

With access to ISP backbone infrastructure – through legal or illegal means – Evasive Panda would be able to intercept and reply to the update requests performed via HTTP, or even modify packets on the fly. In April 2023, Symantec researchers reported on Evasive Panda targeting a telecommunications organization in Africa.

Wrap-up

Ultimately, without further evidence, we cannot prove or discard one hypothesis in favor of the other, given that such capabilities are at hand for Chinese APT groups.

Toolset

MgBot

MgBot is the primary Windows backdoor used by Evasive Panda, which according to our findings has existed since at least 2012 and, as mentioned in this blog post, was publicly documented at VirusBulletin in 2014. It was developed in C++ with an object-oriented design, and has the capabilities to communicate via TCP and UDP, and extend its functionality via plugin modules.

MgBot's installer and backdoor, and their functionality, have not changed significantly since it was first documented. Its chain of execution is the same as described in this report by Malwarebytes from 2020.

MgBot Plugins

MgBot's modular architecture allows it to extend its functionality by receiving and deploying modules on the compromised machine. Table 2 lists the known plugins and their functionality. It is important to note that the plugins don't have unique internal identification numbers; therefore we are identifying them here by their DLL names on disk, which we have never seen change.

Table 2. List of plugin DLL files

Plugin DLL name	Overview
Kstrcs.dll	Keylogger. It only actively logs keystrokes when the foreground window belongs to a process named QQ.exe and the window title matches QQEdit. It's likely target is the Tencent QQ chat application.
sebasek.dll	File stealer. Has a configuration file that enables the collection of files from different sources: HDDs, USB thumb drives, and CD-ROMs; as well as criteria based on the file properties: filename must contain a keyword from a predefined list, file size must be between a defined a minimum and maximum size.
Cbmrpa.dll	Captures text copied to the clipboard and logs information from the USBSTOR registry key.
pRsm.dll	Captures input and output audio streams.
mailLFPassword.dll	Credential stealer. Steals credentials from Outlook and Foxmail email client software.
agentpwd.dll	Credential stealer. Steals credentials from Chrome, Opera, Firefox, Foxmail, QQBrowser, FileZilla, and WinSCP, among others.
qmsdp.dll	A complex plugin designed to steal the content from the Tencent QQ database that stores the user's message history. This is achieved by in-memory patching of the software component KernelUtils.dll and dropping a fake userenv.dll DLL.
wcdbcrk.dll	Information stealer for Tencent WeChat.
Gmck.dll	Cookies stealer for Firefox, Chrome, and Edge.

The majority of the plugins are designed to steal information from highly popular Chinese applications such as QQ, WeChat, QQBrowser, and Foxmail – all of them applications developed by Tencent.

Conclusion

We discovered a campaign that we attribute to the Evasive Panda APT group, targeting users in mainland China, delivering their MgBot backdoor through update protocols of applications from well-known Chinese companies. We also analyzed the plugins of the MgBot backdoor and found the majority of them are designed to spy on users of Chinese software by stealing credentials and information.

IoCs

Files

SHA-1	Filename	Detection	Description
10FB52E4A3D5D6BDA0D22BB7C962BDE95B8DA3DD	wcdbcrk.dll	Win32/Agent.VFT	MgBot information stealer plugir
E5214AB93B3A1FC3993EF2B4AD04DFCC5400D5E2	sebasek.dll	Win32/Agent.VFT	MgBot file stealer plugin.
D60EE17418CC4202BB57909BEC69A76BD318EEB4	kstrcs.dll	Win32/Agent.VFT	MgBot keylogger plugin.
2AC41FFCDE6C8409153DF22872D46CD259766903	gmck.dll	Win32/Agent.VFT	MgBot cookie stealer plugin.
0781A2B6EB656D110A3A8F60E8BCE9D407E4C4FF	qmsdp.dll	Win32/Agent.VFT	MgBot information stealer plugir
9D1ECBBE8637FED0D89FCA1AF35EA821277AD2E8	pRsm.dll	Win32/Agent.VFT	MgBot audio capture plugin.
22532A8C8594CD8A3294E68CEB56ACCF37A613B3	cbmrpa.dll	Win32/Agent.ABUJ	MgBot clipboard text capture plu
970BABE49945B98EFADA72B2314B25A008F75843	agentpwd.dll	Win32/Agent.VFT	MgBot credential stealer plugin.
8A98A023164B50DEC5126EDA270D394E06A144FF	maillfpassword.dll	Win32/Agent.VFT	MgBot credential stealer plugin.
65B03630E186D9B6ADC663C313B44CA122CA2079	QQUrlMgr_QQ88_4296.exe	Win32/Kryptik.HRRI	MgBot installer.

Network

IP	Provider	First seen	Details
122.10.88[.]226	AS55933 Cloudie Limited	2020-07-09	MgBot C&C server.
122.10.90[.]12	AS55933 Cloudie Limited	2020-09-14	MgBot C&C server.

MITRE ATT&CK techniques

This table was built using version 12 of the MITRE ATT&CK framework.

Tactic	ID	Name	Description
Resource Development	T1583.004	Acquire Infrastructure: Server	Evasive Panda acquired servers to be used for C&C infrastructure.
T1587.001	Develop Capabilities: Malware	Evasive Panda develops its custom MgBot backdoor and plugins, including obfuscated loaders.	
Execution	T1059.003	Command and Scripting Interpreter: Windows Command Shell	MgBot's installer launches the service from BAT files with the command net start AppMgmt
T1106	Native API	MgBot's installer uses the CreateProcessInternalW API to execute rundll32.exe to load the backdoor DLL.	
T1569.002	System Services: Service Execution	MgBot is executed as a Windows service.	
Persistence	T1543.003	Create or Modify System Process: Windows Service	MgBot replaces the path of the existing Application Management service DLL with its own.
Privilege Escalation	T1548.002	Abuse Elevation Control Mechanism: Bypass User Account Control	MgBot performs UAC Bypass.
Defense Evasion	T1140	Deobfuscate/Decode Files or Information	MgBot's installer decrypts an embedded CAB file that contains the backdoor DLL.
T1112	Modify Registry	MgBot modifies the registry for persistence.	
T1027	Obfuscated Files or Information	MgBot's installer contains embedded malware files and encrypted strings. MgBot contains encrypted strings. MgBot plugins contain embedded DLL files.	

Tactic	ID	Name	Description
	T1055.002	Process Injection: Portable Executable Injection	MgBot can inject Portable Executable files to remote processes.
Credential Access	T1555.003	Credentials from Password Stores: Credentials from Web Browsers	MgBot plugin module agentpwd.dll steals credential from web browsers.
	T1539	Steal Web Session Cookie	MgBot plugin module Gmck.dll steals cookies.
Discovery	T1082	System Information Discovery	MgBot collects system information.
	T1016	System Network Configuration Discovery	MgBot has the capability to recover network information.
	T1083	File and Directory Discovery	MgBot has the capability of creating file listings.
Collection	T1056.001	Input Capture: Keylogging	MgBot plugin module kstrcs.dll is a keylogger.
	T1560.002	Archive Collected Data: Archive via Library	MgBot's plugin module sebasek.dll uses aPLib to compress files staged for exfiltration.
	T1123	Audio Capture	MgBot's plugin module pRsm.dll captures input and output audio streams.
	T1119	Automated Collection	MgBot's plugin modules capture data from various sources.
	T1115	Clipboard Data	MgBot's plugin module Cbmrpa.dll captures text copied to the clipboard.
	T1025	Data from Removable Media	MgBot's plugin module sebasek.dll collects files from removable media.
	T1074.001	Data Staged: Local Data Staging	MgBot's plugin modules stage data locally on disk.
	T1114.001	Email Collection: Local Email Collection	MgBot's plugin modules are designed to steal credentials and email information from several applications.
	T1113	Screen Capture	MgBot can capture screenshots.
Command and Control	T1095	Non-Application Layer Protocol	MgBot communicates with its C&C through TCP and UDP protocols.
Exfiltration	T1041	Exfiltration Over C2 Channel	MgBot performs exfiltration of collected data via C&C.

26 Apr 2023 - 11:30AM

Sign up to receive an email update whenever a new article is published in our Ukraine Crisis – Digital Security Resource Center

Newsletter

Discussion