Analysis of the APT31 indictment

Identifier: TRR240401

On March 25, 2024, the U.S. Department of Justice (DoJ) released an indictment of seven hackers associated with APT31, a “hacking group in support of China’s Ministry of State Security” (MSS) which has been active for 14 years. On the same day, the Department of Treasury enacted sanctions on several entities listed in the document.

While the U.S. government doesn’t usually disclose investigation methods or IOCs – limiting verifiability of their claims – its attributions have so far never been proven wrong[1]. We gave the indictment a careful read, as such documents always reveal valuable tradecraft information. Key takeaways are:

- APT31 is attributed to the Hubei State Security Department, located in Wuhan;
- Around 2010, APT31 created a front company named “Wuhan XRZ” and used it as a cover for its cyber operations. Another local company, “Wuhan Liuhe” (not accused of being an MSS front), provided support;
- APT31 created and used the RAWDOOR malware, handled a few other malware families used by other Chinese-speaking threat actors, and more recently started using cracked versions of CobaltStrike;
- The group favors a two-band approach to hacking, and goes after subsidiaries, MSPs or spouses of its targets as a means of initial access.

Who is APT31?

APT31, also known as BRONZE VINEWOOD, Zirconium or Judgment Panda, is a long-standing Chinese-speaking threat actor. In the recent years, it garnered attention for:

- Breaking into the network of the Finnish parliament in 2021;
- Repurposing the "EpMe" 0day (CVE-2017-0005) captured from EquationGroup;
- In late 2021, ANSSI reported on a large APT31 campaign against French entities, and noted the uncharacteristic use of compromised SOHO routers as anonymization infrastructure;
- Finally, in 2022, APT31 launched a campaign against Russian media and energy companies, where it leveraged Yandex Cloud as a command and control (C2) infrastructure (as opposed to Dropbox for other campaigns in the West).

Overall, the group is a skilled threat actor, not known to handle cutting-edge 0-day exploits but still capable of devising creative homemade tooling.

The private-public ecosystem

As evidenced in our in-depth review of the I-Soon leak, a significant part of the Chinese cyber-offense apparatus is composed of many small to medium companies conducting hacking operations for the benefit of the state. The APT31 indictment features two such companies:

- Wuhan Liuhe Tiangong Science & Technology Co., Ltd ("Wuhan Liuhe"), founded by one of the defendants;
- Wuhan Xiaoruizhi Science & Technology Co., Ltd ("Wuhan XRZ"), a "front" for the Chinese MSS according to the U.S. DoJ.

Among the seven defendants, four are listed as contractors for Wuhan XRZ, one is the founder of Wuhan Liuhe, and the last two do not have an explicit affiliation. Wuhan XRZ is accused of being responsible of the hacking, while Wuhan Liuhe provided support. Beyond them, the indictment mentions "dozens" of MSS intelligence officers, hackers and support staff (identified by the DoJ but not named in the document) who contributed to the malicious activities.

The document is unclear on why Wuhan Liuhe is only considered to have provided support (and thus wasn't sanctioned), since the one employee cited appears to have maintained victim lists, handled malware and deployed webshells. In any case, the frontier between contractors and intelligence community members appears extremely thin, as one Wuhan XRZ employee developed the RAWDOOR malware (as well as a keylogger and managed the associated infrastructure) while "co-located with an identified MSS officer".

APT31's tactics, techniques and procedures

APT31 appears to have operated using a two-phase methodology, where victims would first receive an email supposedly coming from prominent US journalists. The emails contained legitimate news article excerpts, accompanied by tracking links – which we assume ultimately lead to the original article. Clicking them allowed attackers to obtain preliminary targeting information, such as the type of device on which the email was opened, as well as the public IP address of the recipient. Over 10,000 tracking emails were sent between June and September 2018 only[2].

The threat actor would then use the collected information to engage in direct hacking attempts of the victim's devices based on this information (T1598.003). In particular, the indictment notes that APT31 would **actively target their victims' family members**, so they could go after home routers instead of better protected company

networks. The observation that APT31 focused on SOHO devices is consistent with ANSSI's December 2021 report.

Tooling-wise, APT31 initially used a number of malware families (RAWDOOR, Trochilus, EvilOSX, DropDoor/DropCat[3], etc.), all staged through DLL side-loading. Then the attackers switched to cracked versions of CobaltStrike, an infamous commercial penetration-testing tool. In one case, the U.S. DoJ explains the attackers compromised the subsidiary of a victim (a defense contractor manufacturing flight simulators for the military) before pivoting into the core network from there. The hack involved a local privilege escalation 0-day exploit (we assume CVE-2017-0005, mentioned previously) before exploiting an SQL injection.

While it seems APT31 prefers server-side exploitation (where interactions with the victim are kept to a minimum) for these campaigns, other activities listed in the indictment (for instance, going after Hong Kong's Umbrella Movement activists throughout 2019) show that the actor also relied on spearphishing emails containing malicious attachments or links. The defendants are also accused of creating fake Adobe Flash update pages to deploy the EvilOSX malware (T1036).

A final, less obvious detail contained in the indictment is the fact that APT31 relied on **double infections** for at least some of the victims, allowing them to regain access to the network if the first malware implant was discovered.

About the RAWDOOR malware family

In the list of malware families contained in the indictment, we were not immediately able to associate RAWDOOR with a publicly documented malware strain – save for one mention in an archived transcript of a 2016 iSight report. We nonetheless identified a binary sample (SHA256 `c3056e39f894ff73bba528faac04a1fc86deeec57641ad882000d7d40e5874be`) which was first submitted in September 2015 to an online multi-scanner service, identified as "Rawdoor" by some security products, and "Warood" (a close anagram) by others.

A closer inspection of this malware sample turned out that it is a dropper, deploying either an x86 or x64 payload contained in its resources. The second stage is installed as a service, with uncharacteristic stealth compared to Chinese-speaking threat actor techniques documented for that era:

- The installer inspects the contents of `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SvcHost\netsvcs` and looks for an entry which doesn't have a corresponding service in `HKLM\SYSTEM\CurrentControlSet\Services\`.
- When one is found, it drops its payload as `%WinDir%\Installer\~DF313.msi`. The file is timestomped with the attributes of the system's `calc.exe` file (T1070.006).
- Then it creates the "missing" service with automatic startup, using the command line `%SystemRoot%\system32\svchost.exe -k netsvcs`. The installer edits the corresponding registry key manually to set the `ServiceDll` value to the dropped file.
- Finally, the dropper starts the service, causing the second stage to load.

A summary analysis of the next stage by Microsoft can be found here. We would add to it that the sample we studied uses GitHub as a Command & Control channel[4] (`hxxps://raw.githubusercontent[.]com/willbill4/workspaceer/master/9proxy5/ReadMe.txt`). The corresponding GitHub repository (still online at the time of this writing) received 39 commits between August

5, 2015 and June 6, 2017. The Release folder contains additional binaries, such as a copy of RAWDOOR, likely for update purposes; a PlugX sample; penetration testing utilities such as “netcat”, and other unidentified malware samples.

Considering that samples of the Warood malware family use “RawDoor” as an internal name and in some logging messages, and that some of them contain traces of being compiled on machines in the Chinese language, we assess with high confidence that this malware family is the one referred to in the indictment. Corresponding indicators of compromise are listed in Appendix.

APT31’s flexibility

The indictment notes that the threat actor could change targets extremely quickly, based on political events taking place in the world. It lists a few examples:

- In the context of economic tensions between the U.S. and China, the United States implemented tariffs on imported steel. A day later, as China’s Ministry of Commerce promised a “major response”, APT31 started registering infrastructure impersonating the American Steel Company, then shortly thereafter the International Steel Trade Forum. These domains were immediately used as C2 servers for malware deployed in the network of the American Steel Company.
- Following the nomination of Hong Kong activists for the Nobel Peace Prize in 2018, APT31 went after the Norwegian government as well as a major Norwegian Managed Services Provider (MSP).
- Mid-July 2020, shortly after negative comments from the U.S. administration about China’s territorial claims in the South China Sea, APT31 initiated a spearphishing campaign targeting the U.S. Navy and organizations or think tanks related to it.

Assessment

This indictment contains information consistent with pre-existing knowledge on both APT31 tradecraft, and the nature of the cooperation between public and private Chinese entities on cyber-offense matters. While the U.S. opted not to indict members of the MSS (or if it did, chose not to identify them as such), it is obvious from reading the document that it considers private contractors as intelligence community members.

APT31 has targeted (and in many cases, successfully breached) many high-profile entities in the Western world. The indictment provides a comprehensive view of the group’s interests, ranging from diplomatic intelligence to the theft of trade secrets and even financial data (see full list in appendix). In addition, the U.S. DoJ indicates that the call data records for “millions of Americans” have been acquired by the attackers, which hints at the compromission of at least one telecommunications provider in the country.

It is certain that APT31 is responsible for many more campaigns outside of the United States, not covered by this indictment – particularly in Europe.

Appendix:

Victimology

The following list contains verticals and (where applicable) entities referred to in the indictment. The organizations mentioned were targeted by APT31, but it is not possible to determine which of them were successfully breached from the DoJ's information.

Government	White House
	Department of Justice (including spouses of high-ranking officials)
	Department of Commerce
	Department of Labor
	Department of Transportation
	Department of Treasury
	Department of State
	Congress members from both parties
	Senators from over 10 states
	Senior presidential campaign staff members
	Ambassador in a South-East Asian country
	Political strategists
	Retired national security official
	43 UK parliament members
Defense	U.S. Naval Academy
	U.S. Naval War College's China Maritime Studies
	Contractor designing flight simulators for the U.S. Navy and U.S. Air Force
Industry	American Steel Company
	Various companies in the aerospace sector
Finance & Law	Multiple global law firms throughout the United States
	Unspecified finance, management consulting and financial rating companies
IT & telco	7 Managed Services Providers
	A leading provider of 5G equipment and a 5G integration service company
	A voice technology company
	A company specialized in multi-factor authentication (MFA)
	An undisclosed editor of law-firm software
	Likely one or more ISPs, based on the acquisition of call data records
Research	Laboratory specialized in machine learning
	Various research hospitals and institutes
	Various journalists, academics and policy experts
Civil Society	Democracy activists (in the U.S., Hong Kong)
	Uyghur minority
	Unspecified non-profit organization in Washington
	Interparliamentary Alliance on China

Indicators of Compromise (IOCs)

Please note that the associated APT31 activities are, at best, a few years old. The corresponding IOCs are provided for their historical value. Associated IOCs are also available on our GitHub repository.

File Hashes

```
52238d884006a06e363e546dcfa88c1b2cbdadd80c717e415ac26956900f40bf|RAWDOOR
6f9512a5f2f86938075b14e34928d07cdc78f46ed9401dea799f131f7a3d9644|RAWDOOR
6a9979638d4e4719cfef65bdd6e1d7c0b28b84df9ca73a3bc1e919e9a1df50df|RAWDOOR
```

```
7fda8879c55398434ab0f423b0f1c75658bddd925d90437ad2e6fd8723cb1d78|RAWDOOR
76124bdee942090ec4b5f2a7e08ffe6dae758bc747d6565f6c5941ab81d79044|RAWDOOR
c444a2b741273b5bb86c5197d931cbd3b121043e6e6cb5604b02719415d92b08|RAWDOOR
f332a941d786148a35cec683edb965ea4bbd6ff6bd871880f30dc7d42b922443|RAWDOOR
78a20e644f593acb71d94be96ed1e3a9ba7515be2c50aef844277a9e5c03637a|RAWDOOR
e98d8ae395ec7d2bbc29c21fa2bf79e26ada9d8bd5098487027b32aeae8b03b7|RAWDOOR
e89079508dca536019535bb021ae388a990d9cb64e1e6bd769e6a29ec237d8be|RAWDOOR
fade96ec359474962f2167744ca8c55ab4e6d0700faa142b3d95ec3f4765023b|RAWDOOR
bd3be94afa57936741a5debde1eff537dcd7c7bc79ccfa9739c4614efc424eeb|RAWDOOR
74f7a3b2a5df81eb7b5e0c5c4af8548e61dc37c608dda458b75b58852f2f2cfd|RAWDOOR Dropper
697db25145c2d37f0a521b3ca6b49f1f4d7c3e0c2e57804f5317b3d0b6d242fb|RAWDOOR Dropper
fefa00b0d9a411029f51f34bfa4ed2327559edfcd4fad5cfc1234c1c01a97c5a|RAWDOOR Dropper
c3056e39f894ff73bba528faac04a1fc86deeec57641ad882000d7d40e5874be|RAWDOOR Dropper
```

URLs:

```
hxxps://raw.githubusercontent[.]com/willbill4/workspaceer/|RAWDOOR C2 (hosted by a legitimate service)
hxxp://web10111.googlecode.com/svn/10111.txt|RAWDOOR C2 (hosted by a legitimate service)
```

Yara rules

The provided Yara rules require Yara 4.1.0 (April 26, 2021) and up.

```
rule apt31_rawdoor_dropper
{
    meta:
        description = "Matches the RawDoor dropper"
        references = "TRR240401"
        hash = "c3056e39f894ff73bba528faac04a1fc86deeec57641ad882000d7d40e5874be"
        date = "2024-04-12"
        author = "HarfangLab"
        context = "file"
    strings:
        $service_target = "%SystemRoot%\\system32\\svchost.exe -k netsvcs" ascii
        $service_dispname = "Microsoft .NET Framework NGEN" ascii
        $drop_name = "~DF313.msi" ascii
        $msg1 = "RegOpenKeyEx %s  error:%d\r\n" ascii
        $msg2 = "RegDeleteValue Wow64 . %d\r\n" ascii
        $msg3 = "CreateService %s success! but Start Faile.. %d\r\n" ascii
        $msg4 = "OutResFile to %s%s False!" ascii
        $msg5 = "Can't GetNetSvcs Buffer!" ascii
    condition:
        uint16(0) == 0x5A4D and filesize > 350KB and filesize < 600KB and
        (($service_target and $service_dispname and $drop_name) or 3 of ($msg*))
}
rule apt31_rawdoor_payload
{
```

```
    meta:
        description = "Matches the RawDoor payload"
        references = "TRR240401"
        hash = "fade96ec359474962f2167744ca8c55ab4e6d0700faa142b3d95ec3f4765023b"
        date = "2024-04-12"
        author = "HarfangLab"
        context = "file"
    strings:
        $name = "\r\n================RawDoor %g===============\r\n" ascii
        $key = /SOFTWARE\\Clients\\Netra(u|w)/ ascii
        $cmd1 = "Shell <powershell.exe path>" ascii
        $cmd2 = "Selfcmd <self cmd string>" ascii
        $cmd3 = "Wsrun <process name>" ascii
        $cmd4 = "ping 127.0.0.1 > nul\r\n"
        $cmd5 = "/c netsh advfirewall firewall add rule name=" ascii
        $msg1 = "Allocate pSd memory to failed!" ascii
        $msg2 = "Allocate SID or ACL to failed!" ascii
        $msg3 = "OpenSCManager error:%d" ascii
        $msg4 = "%u:TCP:*:Enabled:%u" ascii
    condition:
        uint16(0) == 0x5A4D and filesize < 200KB and
        (($name and $key) or (3 of ($cmd*) and 3 of ($msg*)))
}
```

[1] It is in fact quite surprising to see that the DoJ is able to attribute specific actions (i.e., writing a piece of malware, managing a victim list or sending a malicious email) to individual defendants, as opposed to their front company.

[2] Email tracking technology is not groundbreaking in itself and is used by advertisers all over the world in their emailing campaigns. The indictment contains references to a commercial service enabling mass email and mail merge, used to send those vast quantities of emails to the victims. Previous reporting by ANSSI indicates this is likely GMass. It follows that the information tracking component was not developed by APT31, but is instead a built-in feature of those services.

[3] Likely the malware strain known as DropboxAES.

[4] This behavior is consistent with APT31's use of public or cloud services for similar purposes. The earliest Rawdoor sample we studied (SHA256 `76124bdee942090ec4b5f2a7e08ffe6dae758bc747d6565f6c5941ab81d79044`, from April 2013) used `googlecode[.]com` for that purpose.

Published on 16 April, 2024 Last update on 22 April, 2024