Open-Source Gh0st RAT Still Haunting Inboxes 15 Years After Release

cofense.com/blog/open-source-gh0st-rat-still-haunting-inboxes-15-years-after-release/

April 24, 2023

Found in Environments Protected By: Proofpoint

By Nathaniel Raymond, Cofense Phishing Defense Center

Gh0st RAT, a decades-old open-source remote administration tool (RAT), recently appeared in phishing campaigns targeting a healthcare organization. Gh0st Remote Administration Tool was created by a Chinese hacking group named C. Rufus Security Team that released it publicly in 2008. The public release of Gh0st RAT source code made it easy for threat actors to obtain and tailor the tool to their needs. Its feature set expanded over the years to include various surveillance, persistence, and information-stealing capabilities:

- Taking full control of the infected machine
- Recording keystrokes in real time with offline logging available
- Accessing live web cam feeds including microphone recording
- Downloading files remotely
- Remote shutdown and reboot
- Disabling user input

Over Gh0st RAT's long life, Chinese nation-state threat actors have used it to breach high-value targets such as governments, embassies, economic targets, and media. One such breach was the operation known as "GhostNet" in 2009, in which a large-scale cyber-attack used Gh0st RAT to conduct surveillance and espionage. The breach impacted the Dalai Lama's Tibetan exile centers in multiple countries.

Although Gh0st RAT was first identified in reports of threat activity almost 15 years ago, it is still actively distributed today. Cofense Intelligence identified an email targeting a European-owned medical technology organization located in China, attempting to deliver Gh0st RAT via an embedded link. The embedded link that hosted the malware was affiliated with Tencent and based in Hong Kong. The sample's command and control (C2) server is also located on the CHINANET Jiangsu province network in the city of Nanjing.

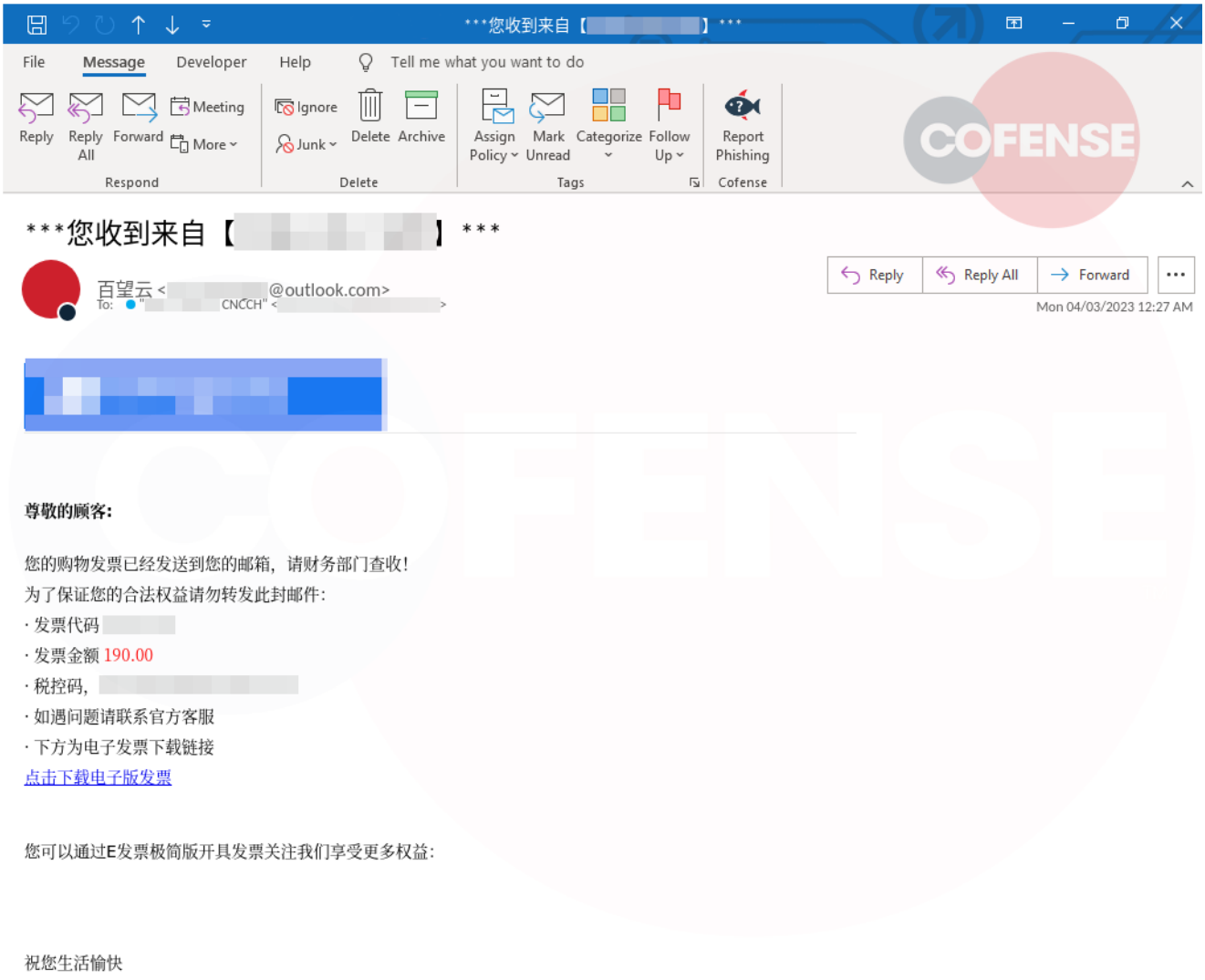

Figure 1: A screenshot of the recent phishing email used to deliver Gh0st RAT via an embedded link.

```
Dear customers

Your shopping invoice has been sent to your mailbox, please check the financial department!
In order to protect your legal rights, please do not forward this email:
· Invoice code REDACTED
· Invoice amount 190.00
· Tax control code, REDACTED
· In case of any problem, please contact the official customer service
· Below is the link to download the electronic invoice
Click to download the electronic invoice

You can issue invoices through the simplified version of E-invoice and follow us to enjoy more benefits
wish you a happy life
```

Figure 2: A translation of the body of the recent Gh0st RAT campaign shows that it used an unpaid invoice as a theme.

Although Ghost RAT has a history of use by nation-state threat actors, Cofense Intelligence does not have conclusive evidence that this recent campaign is associated with known nation-state activity. The activity we observed activity shares certain characteristics with some advanced persistent threat (APT) groups, including APT27, which is known for intellectual property theft against healthcare and technology companies, and is also known for the use of Gh0st RAT. However, since Gh0st RAT's source code is publicly available, it remains plausible that any threat actor could download and modify the code for their own needs. With Chinese universities (including more than one in Nanjing) being heavily involved in training talent for the Chinese defense industry, it is also plausible that students or other threat actors that are at times associated with APT groups may be carrying out independent threat activity using tools they are familiar with.

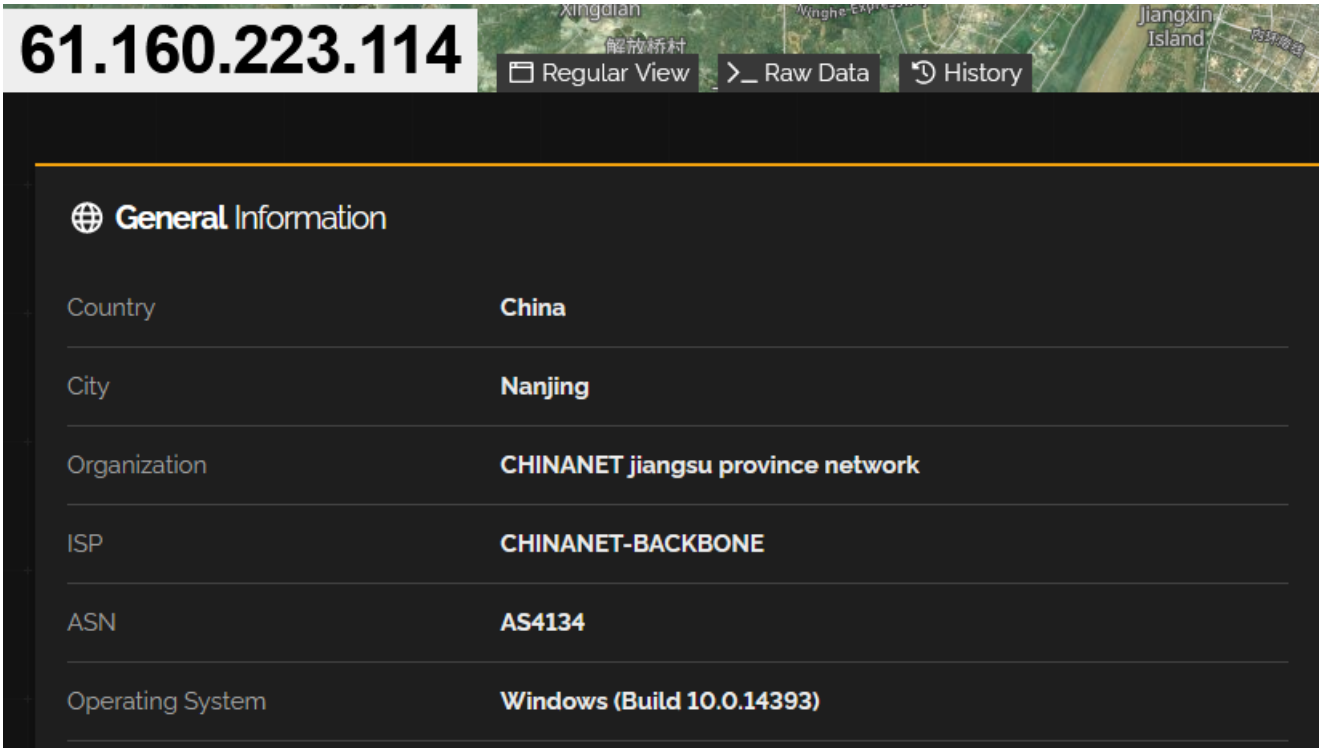

Figure 3: Details of the recent Gh0st RAT sample's C2 server on the network information service Shodan.

Indicators of Compromise
Files
1680478346389.zip MD5: 9e6c45b6b8b20bf3c5959dbba8f27117
LiveUpdate360.dat MD5: f149d3f3ef0361ebe4d346811f29b527
LiveUpdate.exe MD5: 96e4b47a136910d6f588b40d872e7f9d
setting.ini MD5: 91aab4bbe634be62d11d132738c23a82

SqlVersion9.dll MD5: 317f9ff06c076e87e5b1d11242396d5f
ú¿╡ т-╫╚-╖ ó- ├▒ú⌐.exe MD5: 4723a2a8f68c1eaf82809cff29b8e56f
URLs
hxxps://api[.]youkesdt[.]asia/admin/down/hash/79b7c6ed-c4d8-4b36-b1cd-f968e6570010
hxxp://datacache[.]cloudservicesdevc[.]tk/picturess/2023/SqlVersion9[.]dll
hxxp://datacache[.]cloudservicesdevc[.]tk/picturess/2023/Media[.]xml
hxxp://datacache[.]cloudservicesdevc[.]tk/picturess/2023/LiveUpdate360[.]dat
hxxp://datacache[.]cloudservicesdevc[.]tk/picturess/2023/LiveUpdate[.]exe
hxxp://datacache[.]cloudservicesdevc[.]tk/picturess/2023/223[.]114[.]txt
Command and Control
hxxp://61[.]160[.]223[.]114:18076