Hydrochasma: Previously Unknown Group Targets Medical and Shipping Organizations in Asia

symantec-enterprise-blogs.security.com/blogs/threat-intelligence/hydrochasma-asia-medical-shipping-intelligence-gathering

Threat Hunter TeamSymantec

Shipping companies and medical laboratories in Asia are being targeted in a likely intelligence-gathering campaign that relies exclusively on publicly available and living-off-the-land tools.

Hydrochasma, the threat actor behind this campaign, has not been linked to any previously identified group, but appears to have a possible interest in industries that may be involved in COVID-19-related treatments or vaccines.

This activity has been ongoing since at least October 2022. While Symantec, by Broadcom Software, did not see any data being exfiltrated in this campaign, the targets, as well as some of the tools used, indicate that the most likely motivation in this campaign is intelligence gathering.

Attack Chain

The infection vector used by Hydrochasma was most likely a phishing email. The first suspicious activity seen on machines is a lure document with a file name in the victim organization's native language that appears to indicate it was an email attachment:

[TRANSLATED FROM THE ORIGINAL] Product Specification-Freight-Company Qualification Information wps-pdf Export.pdf.exe

Another lure document appears to be mimicking a resume:

[TRANSLATED FROM THE ORIGINAL] [REDACTED] University-Development Engineer.exe

Following initial access on one machine, the attackers were seen dropping Fast Reverse Proxy (FRP), a tool that can expose a local server that is sitting behind an NAT or firewall to the internet. This drops a legitimate Microsoft Edge update file:

%TEMP%\MicrosoftEdgeUpdate.exe

Another file, *%TEMP%\msedgeupdate.dll*, is then seen on victim machines. But this file is actually Meterpreter, a tool that is part of the Metasploit framework and which can be used for remote access.

Other tools that were subsequently seen on this victim's network included:

- **Gogo scanning tool**: An automated scanning engine originally designed for use by red teams.
- **Process Dumper (lsass.exe)**: A tool that allows attackers to dump domain passwords.
- **Cobalt Strike Beacon**: An off-the-shelf tool that can be used to execute commands, inject other processes, elevate current processes, or impersonate other processes, and upload and download files. It ostensibly has legitimate uses as a penetration testing tool but is invariably exploited by malicious actors.
- **AlliN scanning tool**: A pentesting scan tool that can be used for lateral penetration of the intranet.
- **Fscan**: A publicly available hacktool that can scan for open ports and more.
- **Dogz proxy tool**: A free VPN proxy tool.

A shellcode loader and a corrupted portable executable (PE) file were also deployed on this victim's network.

Other tactics, techniques, and procedures (TTPs) observed being used in this campaign included:

- **SoftEtherVPN**: The presence of this tool was what first prompted Symantec researchers to investigate this activity. It is free, open-source, and cross-platform VPN software.
- **Procdump**: Microsoft Sysinternals tool for monitoring an application for CPU spikes and generating crash dumps, but which can also be used as a general process dump utility.
- **BrowserGhost**: A publicly available tool that can grab passwords from an internet browser.
- **Gost proxy**: A tunneling tool.
- **NtlmrelayRelay**: An NTLM relay attack allows an attacker to intercept validated authentication requests in order to access network services.
- **Task Scheduler**: Allows tasks to be automated on a computer.
- **Go-strip:** Used to make a Go binary smaller in size.
- **HackBrowserData:** An open-source tool that can decrypt browser data.

The tools deployed by Hydrochasma indicate a desire to achieve persistent and stealthy access to victim machines, as well as an effort to escalate privileges and spread laterally across victim networks.

While Symantec researchers didn't observe data being exfiltrated from victim machines, some of the tools deployed by Hydrochasma do allow for remote access and could potentially be used to exfiltrate data. The sectors targeted also point towards the motivation behind this attack being intelligence gathering.

The lack of custom malware used in this attack is also notable. Relying exclusively on living-off-the-land and publicly available tools can help make an attack stealthier, while also making attribution more difficult. Symantec did not see evidence to link this activity to a known actor, prompting us to create the new actor identity of Hydrochasma for those behind this activity.

Protection/Mitigation

For the latest protection updates, please visit the Symantec Protection Bulletin.

Indicators of Compromise

If an IOC is malicious and the file available to us, Symantec Endpoint products will detect and block that file.

File Indicators

SHA256

409f89f4a00e649ccd8ce1a4a08afe03cb5d1c623ab54a80874aebf09a9840e5 – Fast Reverse Proxy

47d328c308c710a7e84bbfb71aa09593e7a82b707fde0fb9356fb7124118dc88 – GoGo Scanning Tool

6698a81e993363fab0550855c339d9a20a25d159aaa9c4b91f60bb4a68627132 – Dropper

7229bd06cb2a4bbe157d72a3734ba25bc7c08d6644c3747cdc4bcc5776f4b5b9 – Process Dumper (lsass.exe)

72885373e3e8404f1889e479b3d46dd8111280379c4065bfc1e62df093e42aba – Fast Reverse Proxy

72bc8b30df3cdde6c58ef1e8a3eae9e7882d1abe0b7d4810270b5a0cc077bb1a – Cobalt Strike Beacon

7b410fa2a93ed04a4155df30ffde7d43131c724cdf60815ee354988b31e826f8 – Fast Reverse Proxy

7f0807d40e9417141bf274ef8467a240e20109a489524e62b090bccdb4998bc6 – Process Dumper (lsass.exe)

8c0f0d1acb04693a6bdd456a6fcd37243e502b21d17c8d9256940fc7943b1e9a – Cobalt Strike Beacon

8e32ea45e1139b459742e676b7b2499810c3716216ba2ec55b77c79495901043 – Fast Reverse Proxy

981e5f7219a2f92a908459529c42747ac5f5a820995f66234716c538b19993eb – GoGo Scanning Tool

9ebd789e8ca8b96ed55fc8e95c98a45a61baea3805fd440f50f2bde5ffd7a372 – Fast Reverse Proxy

9f5f7ba7d276f162cc32791bfbaa0199013290a8ac250eb95fd90bc004c3fd36 – Cobalt Strike Beacon

a0f5966fcc64ce2d10f24e02ae96cdc91590452b9a96b3b1d4a2f66c722eec34 – AllIn Scanning Tool

cb03b5d517090b20749905a330c55df9eb4d1c6b37b1b31fae1982e32fd10009 – Fscan

d1c4968e7690fd40809491acc8787389de0b7cbc672c235639ae7b4d07d04dd4 – Shellcode Loader

de01492b44372f2e4e38354845e7f86e0be5fb8f5051baafd004ec5c1567039f – Cobalt Strike Beacon

e378d8b5a35d4ec75cae7524e64c1d605f1511f9630c671321ee46aa7c4d378b – PE File

eba22f50eedfec960fac408d9e6add4b0bd91dd5294bee8cff730db53b822841 – Dropper

fc4b5f2ee9da1fe105bb1b7768754d48f798bf181cbc53583387578a5ebc7b56 – Dogz Proxy Tool

02fe00ffd1b076983f3866c04ca95c56cef88c2564fabb586e11e54986e87ba7

084d1fc4236011d442801e423485c8e58f68dc14ec0a8b716fa0fd210de43dda

1744fac628262aa0cf3810bd5168375959be41764c8ca2fa41950a7b1f8f2fad

1d087f6a17227769bcebc799a2cdf1bb2a8fdf6ba560d21a88bb71f1c213a42c

327fc116f8f48f97292184bb50cb3db418f368b3e2a0fb41267ba40254a35a89

3516f94b0fb57e93c6659d813cbf5fb3617dea7a667c78cb70a1914306327906

41b6d26926706bb68530ddff234f69757e3bbef91c47eb0255313ed86cb3f806

44223e5abd106c077908f03c93b8c8baee7d630f1718f9750f16b786cf88fd06

553e0763cf3a938b5754c9d89939a118abe0b235e4be6920c34f562bd758e586

5a62abc0a2208679e414cc71d1f36ffa14b48df2b73ac520e45d557ad77dd004

6770f815480d7cfa0a6fc8599c08ca6013f608d257a2121233e77374e21c53f8

6cb815863088a0ad367b2a525a572323600596f6875a79536aee57202ef24fd5

6f017ad84d0d06f50b6213a0742838b5ec510f3d06f96e0300048f2da6a35c41

7394ab0ed6d1f62e83fc5f8f1eb720ddd07cbd2bcdf6a00b9b63ef6018fa5f90

7800a4fb0cbdf29815c521ea8b00a23e28d7eb365653f2afcfb5572622727218

7f6a1d6950a9464f27d8651a267563d4630d223bf7ac66851917a57f8fac6550

84502fbe3e5172c39e9a97734e6caac79255abffcb55c22752620d908ff33940

916b63b88de2549c4a5c8e13d51df4cf6996067ae30f24c8bb35c66db7c061df

968b28f7d6abb845f2cc7efa93cdcf7660585e22d589267695726de13afea260

9e8b5a84ad108a761619ca040788dcbf07996a9101cecc5c30ba61f9a06945c1

b53d0a43ea91b3c80bc6c87c0c6946816c38876b2cb2f6f772afe94c54d3ad30

b5c4f420067499522b748a34161ad6e140a7f30ab0b8fa63feef760c5e631679

d0ae66022929c17f31ddf98d88817f0aa70a56ce2ff2df9595b8889c2d3d7e31

d92c50a91bd5b2f06f41a9a5f9937e50b78658d46e3cd04bc3a85f270ce288c2

dc3b714fd6f93c0c0cd2685b6b8cd551896855474bdd09593b8c6b4b7ab6bac2

e7684a4984d9d82115c5cc1b43b9f63a11e7ed333a4e2d92dc15b6e931634bf4

ebc3dabf0a2dafb0790be6dbb4d3509b5ce1259b955172910618a32627b3b668

ee9aefde33ed48d16ecb1c41256fc7d93ddfa8bedfa59b95e8810282ac164d0d

f35b206fe10ad3f57d9c4ecf71a2d2cc06d7c7fe905e567b989f72f147da99dc

f73738e6e33286657cda81f618a74b74745590915a8f4451e7c00473cbe89e1d

fc8a67b80b0b0ecd10dfd90820ffc64923b94c32b04dbb6929a79b9ce027563c

ffdcf74968805e9cc897ca932e4da0f22ea7b3e9b96fcc9082c0c5300ae4cb0d

Network Indicators

IPs

39.101.194[.]61 – Cobalt Strike Beacon C&C

47.92.138[.]241 – Cobalt Strike Beacon C&C

106.14.184[.]148

180.119.234[.]147

Domains

alidocs.dingtalk[.]com.wswebpic[.]com – Cobalt Strike Beacon C&C

csc.zte[.]com.cn.wswebpic[.]com – Cobalt Strike Beacon C&C

taoche[.]cn.wswebpic[.]com – Cobalt Strike Beacon C&C

URLs

hxxp://47.92.138[.]241:8090/update.exe

hxxp://47.92.138[.]241:8000/agent.exe

hxxp://47.92.138[.]241:8000/update.exe

hxxp://47.92.138[.]241:8000/ff.exe

hxxp://47.92.138[.]241:8000/aa.exe

hxxp://47.92.138[.]241:8000/runas.exe

hxxp://47.92.138[.]241:8090/a.exe

hxxp://47.92.138[.]241:8000/t.exe

hxxp://47.92.138[.]241:8000/po.exe

hxxp://47.92.138[.]241:8080/t.exe

hxxp://47.92.138[.]241:8899/t.exe

hxxp://47.92.138[.]241:8000/logo.png

hxxp://47.92.138[.]241:8080/t.png

hxxp://47.92.138[.]241:8000/frp.exe

About the Author

Threat Hunter Team

Symantec

The Threat Hunter Team is a group of security experts within Symantec whose mission is to investigate targeted attacks, drive enhanced protection in Symantec products, and offer analysis that helps customers respond to attacks.