Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

Water Orthrus Targets Chinese Users with CopperStealth and CopperPhish

Date of Publication	Admiralty Code	TA Number
May 16, 2023	A1	TA2023231

Summary

Attack began: March 8, 2023
Attack Regions: China
Malware: CopperStealth and CopperPhish
Threat Actor: Water Orthrus
Attack: Water Orthrus, a threat actor active since 2021, has recently launched two new campaigns, CopperStealth and CopperPhish, where CopperStealth employs rootkit techniques to inject malware disguised as free software and target Chinese users, while CopperPhish globally distributes a phishing kit through PPI networks, demonstrating the actor's evolving focus from personal information to cryptocurrency and now credit card details.

Attack Regions

Attack Details

#1 Since 2021, a threat actor known as Water Orthrus has been distributing the CopperStealer malware through pay-per-install networks. The malware has undergone several upgrades and modifications, serving various purposes like injecting network advertisements, stealing personal information, and pilfering cryptocurrency. Water Orthrus is believed to be connected to the Scranos threat campaign reported in 2019.

#2 In March 2023, two new campaigns associated with Water Orthrus were observed. The first campaign, named CopperStealth, delivered the malware disguised as free software through a popular Chinese software sharing website, targeting Chinese users. CopperStealth's infection chain involved dropping and loading a rootkit, which injected its payload into system processes. The rootkit blocked access to certain registry keys, prevented the execution of specific executables and drivers, and employed other evasion techniques.

#3 The second campaign, called CopperPhish, was detected in April 2023. Unlike CopperStealth, CopperPhish was distributed globally through PPI networks using free anonymous file sharing websites. CopperPhish is a phishing kit that utilizes two processes for persistence and verifies credentials and a confirmation code before considering the phishing attempt successful.

#4 Both campaigns exhibit similarities to previous campaigns associated with Water Orthrus, such as the use of the same crypter, Data Encryption Standard (DES) with specific key and initialization vector, similar DLL export function names, and comparable mutex naming conventions.

#5 The findings indicate that Water Orthrus has refined its malware and adapted its attacks to different targets. The CopperStealth campaign focused on installing a rootkit, while CopperPhish aimed to phish credit card information. The actor's shifting interests have evolved from personal information to cryptocurrency and now target credit card details.

Recommendations

Implement robust email security measures: As Water Orthrus employs phishing techniques, it's crucial to strengthen your email security. Consider implementing an advanced email security solution that can detect and block phishing emails, malicious attachments, and suspicious links. Look for features like email authentication (SPF, DKIM, DMARC), sandboxing, and machine learning algorithms for improved threat detection.

Enforce strict password policies and MFA: Password security remains a vital aspect of protecting against various threats. Ensure that your organization has a strict password policy in place, encouraging employees to use strong, unique passwords and change them regularly. Additionally, enable multi-factor authentication (MFA) for all user accounts, particularly those with privileged access, to add an extra layer of protection against unauthorized access attempts.

Conduct regular security awareness training: Educate your employees about the latest phishing techniques, social engineering tactics, and best practices for identifying and handling suspicious emails. Offer regular security awareness training sessions and provide employees with simulated phishing exercises to reinforce good security habits. By creating a culture of vigilance and awareness, you can significantly reduce the risk of falling victim to Water Orthrus's phishing campaigns.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	TA0008 Lateral Movement
TA0009 Collection	TA0010 Exfiltration	T1566 Phishing	T1195 Supply Chain Compromise
T1218 System Binary Proxy Execution	T1218.002 Control Panel	T1204 User Execution	T1202 Indirect Command Execution

T1070 Indicator Removal	**T1033** System Owner/User Discovery	**T1041** Exfiltration Over C2 Channel	**T1071** Application Layer Protocol
T1078 Valid Accounts	**T1068** Exploitation for Privilege Escalation	**T1542** Pre-OS Boot	**T1542.003** Bootkit
T1027 Obfuscated Files or Information	**T1020** Automated Exfiltration	**T1087** Account Discovery	**T1110** Brute Force
T1059 Command and Scripting Interpreter	**T1059.001** PowerShell	**T1082** System Information Discovery	**T1552** Unsecured Credentials
T1552.001 Credentials In Files	**T1021** Remote Services	**T1056** Input Capture	**T1046** Network Service Discovery
T1047 Windows Management Instrumentation			

Indicators of Compromise (IOCs)

TYPE	VALUE
URLs	hxxp://cnzz[.]fnxitong[.]com:99/gg[.]html hxxp://chromei[.]org/tj/ hxxp://so[.]fnxitong[.]com:99/tongji[.]php?u=e002 hxxp://so[.]fnxitong[.]com:99/tongji[.]php?u=001 hxxp://cnzz[.]fnxitong[.]com:99/gg[.]txt hxxp://chromei[.]org/encode[.]txt hxxp://up[.]chromei[.]org/e002[.]txt hxxp://www[.]chromel[.]cn/encode[.]txt hxxps://0zpt4[.]za[.]com/ hxxps://3hdr0[.]za[.]com/
SHA256	699873a949ca1e3a15f8428d1e28e3bdf7b95ec1606e10785f3f51b118e2669e dda6bc4618cd6f723d6ad5f45f171a075c208b5b2693a35f24dd6607a3f167f0 7e3f5a8f6fc490736ba7e04389cf83d9ea47a5079e63901300e2dec79c1f77ab 1fd3c8d5ec7043fb01ea9d9985075d0b014f7153e88cd56d267fb10f1f979a1c 50fae4fe4a258854c629a3dd24262e1a35a09d317f2d1b7bb31d5a81a237c258

TYPE	VALUE
SHA256	8a21eae144a23fffd35f8714964ff316caaa37fe464e8bbc143f4485119b5575 293a2adf60a94437cc0f92545b7caabdaed0a63007b51e2b3d449cdb1e00f5a8 6c3995155e0e5cbb17e6f71b8d8b89d4dfc77849e869da7901a79053e8e8232b 5558eaebeeeb4c5c731b531305e7c97c9cf1b1449b0466f46430aa0549c256e9 ad5f59c497f423a07cfb4affc82aac408eafeeefef22f8ba25cabff2ff9911754 636772857bd9b88d5b530586c7008f48e61ec429fb50a82019d0505dcf994930 7246dbf235f66034bd7042408f01b8670c3f45d39082fcbf5b893d7952614833 73fd83a9eb267fed5a3178b75a9bff0bac9e0864daed830fddf6a8686c286cbb 7fd6cb3e1648dd9d1994c65762826772ae32dc58fbc7ac51179a0b3526f1395f e3f31eabaa0b3bebe0c5152fc6097a8fbf1c6fd9e57d06fe8e9bd8860e8f07a6 033ba1740ba105bf4a5081f438f46f1d7ad17a175aab132bd844edcf8e30949f ed88b019b3a8346c89aaf6ba7ce6c6be0b9a88c121312f3db9b6ebd776a9af5a ecdd5adb40297ec29c0e8a8f50223069db3d32c2a1d223adfb52c3a695d41fa2 f916f4d1d8c1df0d31b8d18b7c94109b4303412880538f64ec3eb2e257732ead 53f4306d30b4f7b731c0cd7be6df39f02613fb4c0e9b5aa85f754e145dca080c 139f8412a7c6fdc43dcfbbcdba256ee55654eb36a40f338249d5162a1f69b988 5b932eab6c67f62f097a3249477ac46d80ddccdc52654f8674060b4ddf638e5d 6994b32e3f3357f4a1d0abe81e8b62dd54e36b17816f2f1a80018584200a1b77 32882949ea084434a376451ff8364243a50485a3b4af2f2240bb5f20c164543d 50819a1add4c81c0d53203592d6803f022443440935ff8260ff3b6d5253c0c76 770f33259d6fb10f4a32d8a57d0d12953e8455c72bb7b60cb39ce505c507013a 86047bb1969d1db455493955fd450d18c62a3f36294d0a6c3732c88dfbcc4f62

TYPE	VALUE
SHA256	06c5ebd0371342d18bc81a96f5e5ce28de64101e3c2fd0161d0b54d8368d2f1f 6661320f779337b95bbbe1943ee64afb2101c92f92f3d1571c1bf4201c38c724 f9f2091fccb289bcf6a945f6b38676ec71dedb32f3674262928ccaf840ca131a e6f764c3b5580cd1675cbf184938ad5a201a8c096607857869bd7c3399df0d12 e1cb86386757b947b39086cc8639da988f6e8018ca9995dd669bdc03c8d39d7d 4734a0a5d88f44a4939b8d812364cab6ca5f611b9b8ceebe27df6c1ed3a6d8a4 ea50f22daade04d3ca06dedb497b905215cba31aae7b4cab4b533fda0c5be620 fa9abb3e7e06f857be191a1e049dd37642ec41fb2520c105df2227fcac3de5d5 f936ec4c8164cbd31add659b61c16cb3a717eac90e74d89c47afb96b60120280 a292fd3792ef81f3a3afd73c5b19878677e0293528e646e244ef50a36c4a0fb2 8b141803aeaa4f696fb19711d45a2628c73476c893ac1ba7967eb8d84862ea9a ac4bcb31d35428d8147d413d3354b9fdf70d9e9f3463ead04783805fdd306d86 04d2cb7d5f0e28797c1fde9036f06535040c223ecd66828e21c55971241adbbf bf5ae3846ada31fdf91f7d9c03c54dd10598571a5a24ed96c582a6a6fe20006f e257b8efdb3719bf21ed15d5abb30b0cbdbf9027a3db17ad0baca319eec13889 49337a65b01dd6e634456bca17ca28118a8126e4706d92b4673afe1c9cfea638 4934e4990928dbec77463f383b693f4f4a9fc40256e72a36e98c292722b84cf1 48211c6f957c2ad024441be3fc32aecd7c317dfc92523b0a675c0cfec86ffdd9 8c01578891b08d168c1919c4f2ed4fdac991e063263bbb63963ea616f5d5333e 39c9f743528eb317340cdd53a65630785b1168f6f0a6b253ae2518fb450f0b81 28d1d1c6fb23ef5f92b16e2701c49bb34b4a81af11f95ff5674d291c5ffb3b28 07cccf04854a58e43a5043e240b662f84ac512b2d2432b1b7e4cd5465d1dde33

TYPE	VALUE
SHA256	036a689038dfaa195c899d57a4d3fdcf5f99b91bdbf9739a4d05f9bd1dcfe15e 65a632de69bcb62c8f344a9cc0951d3c599301ca6d8aed66bbdab9f1b977799a 971259ae3eb7dc843c6872b22154e5cf74e48ca35fb895145df63fa50e8e8792 58eb8b6fd34406316438e2e17ed3c44b6c26695b28c71db7b062a63a116ee33b 0a596289cb9c6dcb065d96fb33c1e9509f62ff42b00a0d679bb8b9e64dce8ea5 fcf49a50a3b86adeea6b1cfbb0d86dfed774673a5900570878197f822f6f2126 8c01578891b08d168c1919c4f2ed4fdac991e063263bbb63963ea616f5d5333e 6f52f36d84ea04d00f307d5aafedcda98118d140c1ac1af0525ecb374c0f5cf2 688de5bbd2cb1e5556304002c1b7f5fdfe147251217f93b8733017161a834fa5 1a1a70fd2c5a012c4e8547713a3abf1dc2dbd05a81ab1fcca4ab1ad71ad36979 15430150c081728440618aac046cc1d50a4391b55fa7f8fa66325d9b462e57c3 acac571f03810d6e8408d4df25fda741cf492c7d842113155034da1f871c10ea F340e0ef5f90024b9626a83c2c1eed2011417372073088169d7c2c7ec842f228 a5f00b52c99b951009334c6c52524c4e494c8ee77da1340a623a35a35e96b935 00ff5f2af303cee7ede802b8a013f415bc69caa023330143df746b9b23aa60fd Dd3ffec50a0ef7434b85f85330cebb9a2afa2123bed19ac39179806bacf48775 Bff741d972e1dac7fa1197ac9365106b49bd07cea868d69c660aa569fe75f005 bb2422e96ea993007f25c71d55b2eddfa1e940c89e895abb50dd07d7c17ca1df

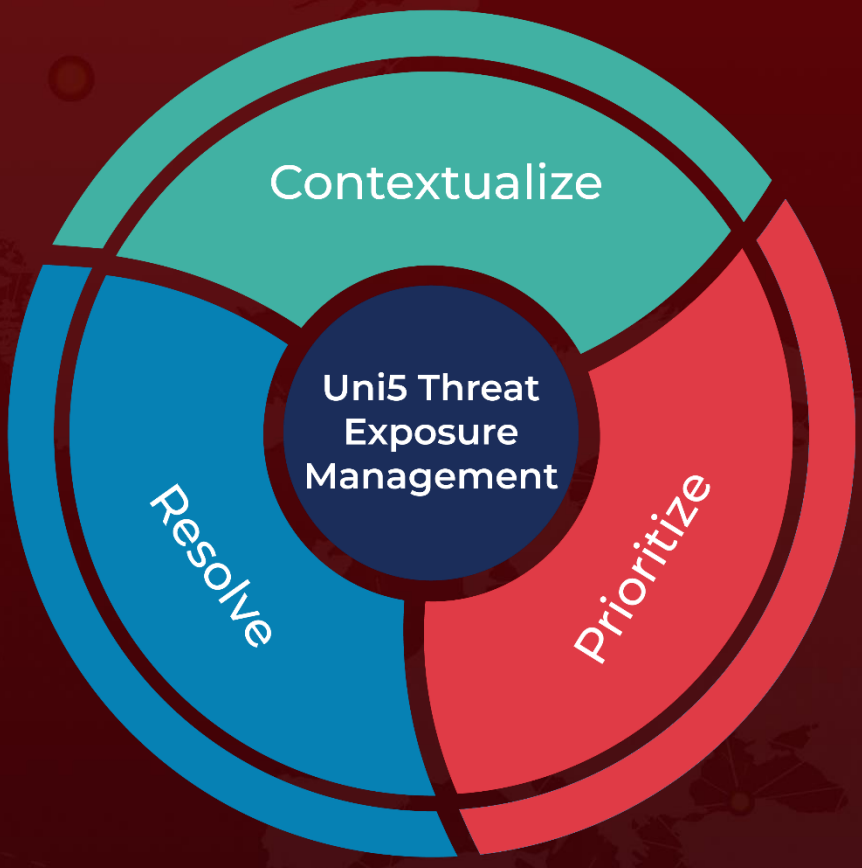
References

https://www.trendmicro.com/en_us/research/23/e/water-orthrus-new-campaigns-deliver-rootkit-and-phishing-modules.html

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

May 16, 2023 • 6:30 AM

More at www.hivepro.com