Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ACTOR REPORT

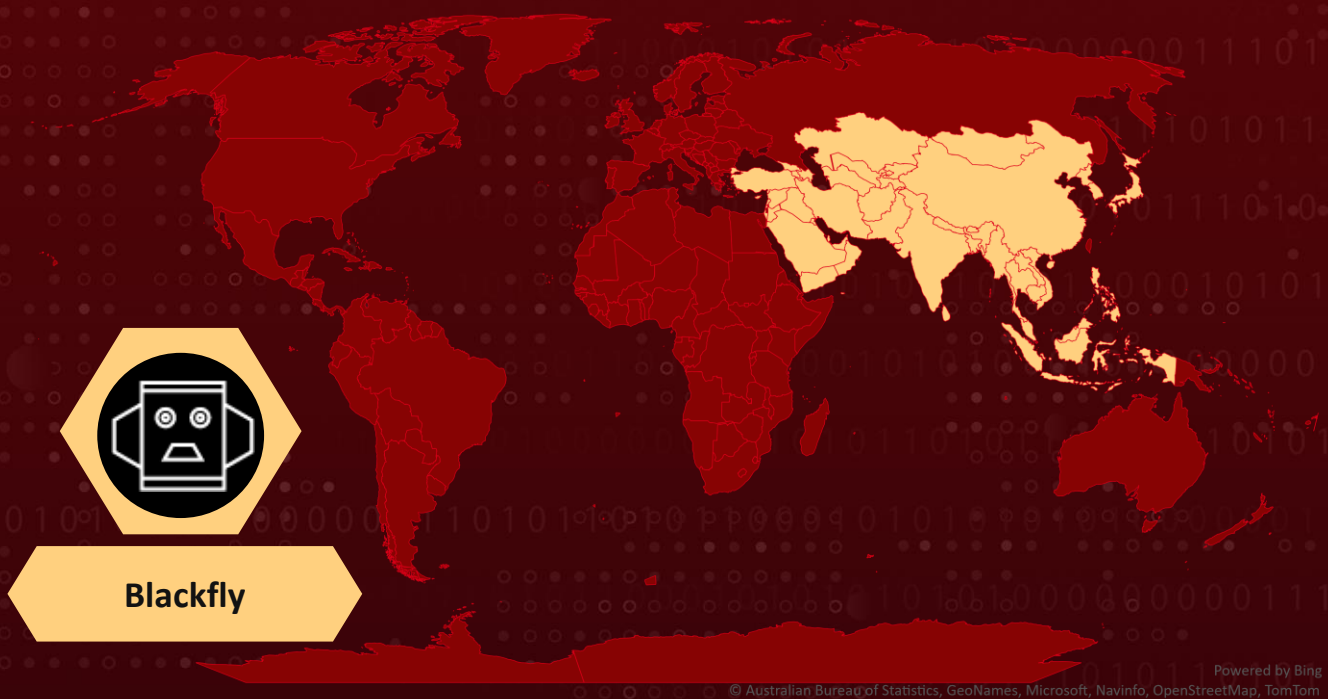
Blackfly Chinese APT targets Asian conglomerate in materials sector

Date of Publication	Admiralty code	TA Number
March 01, 2023	A1	TA2023109

Summary

First Appearance: 2010
Actor Name: Blackfly (APT41, Wicked Panda, Winnti Group)
Target Region: Asia
Target Sectors: Materials, composites semiconductor, telecoms, materials manufacturing, pharmaceutical, media and advertising, hospitality, natural resources, fintech, and food.

Actor Map



Actor Details

#1

The Blackfly espionage group, also known as APT41, Winnti Group, or Bronze Atlas, has been targeting multiple subsidiaries of an Asian conglomerate operating in the materials and composites sector, suggesting that the group may be trying to steal intellectual property. Blackfly is one of the longest-known Chinese advanced persistent threat (APT) group and has been active since at least 2010.

#2

The group was initially known for attacking the computer gaming industry, but it has since expanded its targets to a wide range of sectors, including semiconductor, telecoms, materials manufacturing, pharmaceutical, media and advertising, hospitality, natural resources, fintech, and food. Despite being the subject of a US indictment, Blackfly has continued to mount attacks, seemingly undeterred by the publicity it has received. The group's latest activity shows that it has been relying more on open-source tools than its usual custom malware, which helps it avoid detection and attribution.

#3

The use of open-source tools is a trend that has been seen among other threat groups targeting the region. While the group's technical sophistication has remained consistent, it has been regularly refreshing its toolset in a bid to stay ahead of detection. The group has been associated with a second Chinese APT group called Grayfly, and despite being indicted by the US, Blackfly continues to operate and target intellectual property across different industries.

Actor Group

NAME	ORIGIN	TARGET REGIONS	TARGET INDUSTRIES
Blackfly (APT41, Wicked Panda, Winnti Group)	China	Asia	Materials, composites semiconductor, telecoms, materials manufacturing, pharmaceutical, media and advertising, hospitality, natural resources, fintech, and food.
	MOTIVE		
	Information theft and espionage		

Recommendations

Security Leaders

Phishing simulations and routine education and awareness training and communications rarely account for MFA fatigue and web browser hygiene. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize and block all indicators attributed to the threat actor through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.
- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' & 'Indicators of Compromise (IoC)' on the following pages.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0005 Defense Evasion	TA0011 Command and Control	TA0007 Discovery
T1583.001 Domains	T1083 File and Directory Discovery	T1105 Ingress Tool Transfer	T1057 Process Discovery
T1014 Rootkit	T1553.002 Code Signing	T1583 Acquire Infrastructure	T1553 Subvert Trust Controls
T0882 Theft of Operational Information	T1003 OS Credential Dumping	T1113 Screen Capture	T1055.012 Process Hollowing
T1055 Process Injection	T1090 Proxy		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA 256	cf6bcd3a62720f0e26e1880fe7ac9ca6c62f7f05f1f68b8fe59a4eb47377880 e1e0b887b68307ed192d393e886d8b982e4a2fd232ee13c2f20cd05f91358596 a3078d0c4c564f5efb1460e7d341981282f637d38048501221125756bc740aac 714cef77c92b1d909972580ec7602b0914f30e32c09a5e8cb9cb4d32aa2a2196 192ef0dee8df73eec9ee617abe4b0104799f9543a22a41e28d4d44c3ad713284 caba1085791d13172b1bb5aca25616010349ecce17564a00cb1d89c7158d6459 452d08d420a8d564ff5df6f6a91521887f8b9141d96c77a423ac7fc9c28e07e4 1cc838896fbaf7c1996198309fbf273c058b796cd2ac1ba7a46bee6df606900e 4ae2cb9454077300151e701e6ac4e4d26dc72227135651e02437902ac05aa80d 560ea79a96dc4f459e96df379b00b59828639b02bd7a7a9964b06d04cb43a35a b28456a0252f4cd308dfb84eeaa14b713d86ba30c4b9ca8d87ba3e592fd27f1c a3acb9f79647f813671c1a21097a51836b0b95397ebc9cd178bc806e1773c864 5e51bdf067e5781d2868d97e7608187d2fec423856dbc883c6f81a9746e99b9f d4e1f09cb7b9b03b4779c87f2a10d379f1dd010a9686d221c3a9f45bda5655ee f138d785d494b8ff12d4a57db94958131f61c76d5d2c4d387b343a213b29d18f 88113bebc49d40c0aa1f1f0b10a7e6e71e4ed3ae595362451bd9dcebcf7f8bf4 498e8d231f97c037909662764397e02f67d0ee16b4f6744cf923f4de3b522bc1 100cad54c1f54126b9d37eb8c9e426cb609fc0eda0e9a241c2c9fd5a3a01ad6c

References

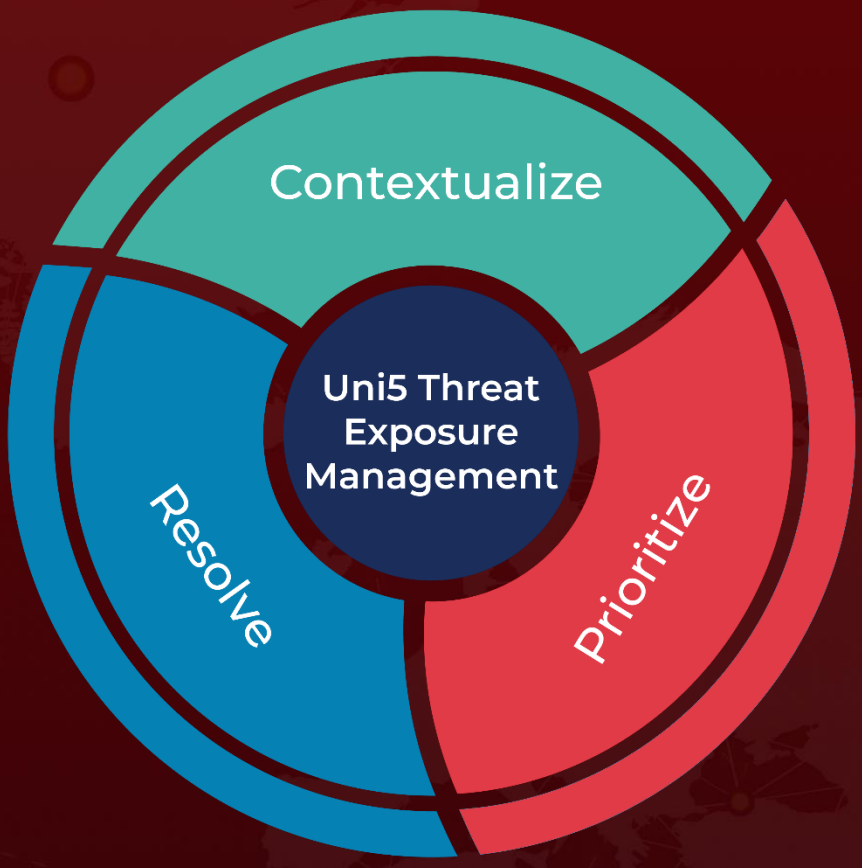
https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/blackfly-espionage-materials

https://www.darkreading.com/endpoint/china-blackfly-targets-materials-sector-relentless-quest-ip

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

March 01, 2023 . 1:00 AM

© 2023 All Rights are Reserved by HivePro

More at www.hivepro.com