# Blackfly: Espionage Group Targets Materials Technology

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

The Blackfly espionage group (aka APT41, Winnti Group, Bronze Atlas) has continued to mount attacks against targets in Asia and recently targeted two subsidiaries of an Asian conglomerate, both of which operate in the materials and composites sector, suggesting that the group may be attempting to steal intellectual property.

## Current Blackfly toolset

The following tools were used in attacks during late 2022 and early 2023:

- **Backdoor.Winnkit**
  SHA256: caba1085791d13172b1bb5aca25616010349ecce17564a00cb1d89c7158d6459
  SHA256: cf6bcd3a62720f0e26e1880fe7ac9ca6c62f7f05f1f68b8fe59a4eb47377880a
  SHA256: e1e0b887b68307ed192d393e886d8b982e4a2fd232ee13c2f20cd05f91358596
  SHA256: a3078d0c4c564f5efb1460e7d34198128 2f637d3804850122125756bc740aac
  SHA256: 714cef77c92b1d90997258 0ec7602b0914f30e32c09a5e8cb9cb4d32aa2a2196
  SHA256: 192ef0dee8df73eec9ee617abe4b0104799f9543a22a41e28d4d44c3ad713284
  Rootkit driver known to be associated with Blackfly

- **Credential-dumping tool**
  SHA256: 100cad54c1f54126b9d37eb8c9e426cb609fc0eda0e9a241c2c9fd5a3a01ad6c
  Creates a dump of credentials from lsass.exe in C:\windows\temp\1.bin.

- **Screenshotting tool**
  SHA256: 452d08d420a8d564ff5df6f6a91521887f8b9141d96c77a423ac7fc9c28e07e4
  Screenshots all open windows and saves them as .jpg files.

- **Process-hollowing tool**
  SHA256: 1cc838896fbaf7c1996198309fbf273c058b796cd2ac1ba7a46bee6df606900e
  Injects shellcode in C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted. The shellcode is a simple "Hello World" alert message.

- **SQL tool**
  SHA256: 4ae2cb94540773 00151e701e6ac4e4d26dc7222713565 1e02437902ac05aa80d
  SQL client tool used to query SQL databases.

- **Mimikatz**
  SHA256:
  560ea79a96dc4f459e96df379b00b59828639b02bd7a7a9964b06d04cb43a35a
  SHA256: b28456a0252f4cd308dfb84eeaa14b713d86ba30c4b9ca8d87ba3e592fd27f1c
  Publicly available credential-dumping tool.

- **ForkPlayground**
  SHA256: a3acb9f79647f813671c1a21097a51836b0b95397ebc9cd178bc806e1773c864
  Proof-of-Concept application to create a memory dump of an arbitrary process using the ForkLib.

- **Proxy configuration tool**
  SHA256: 5e51bdf067e5781d2868d97e7608187d2fec423856dbc883c6f81a9746e99b9f
  SHA256: d4e1f09cb7b9b03b4779c87f2a10d379f1dd010a9686d221c3a9f45bda5655ee
  SHA256: f138d785d494b8ff12d4a57db94958131f61c76d5d2c4d387b343a213b29d18f
  Configures proxy settings by injecting into: C:\Windows\system32\svchost.exe -k LocalSystemNetworkRestricted.

- **Proxy configuration tool**
  SHA256: 88113bebc49d40c0aa1f1f0b10a7e6e71e4ed3ae595362451bd9dcebcf7f8bf4
  SHA256: 498e8d231f97c03790966276439 7e02f67d0ee16b4f6744cf923f4de3b522bc1
  This tool requires a file called conf.dat to run properly, located at: c:\users\public\conf.dat. Conf.dat contains the configuration to set up proxy settings.

## Longstanding APT group

Blackfly is one of the longest known Chinese advanced persistent threat (APT) groups, active since at least 2010. Early attacks were distinguished by the use of the PlugX/Fast (Backdoor.Korplug), Winnti/Pasteboy (Backdoor.Winnti), and Shadowpad (Backdoor.Shadowpad) malware families. The group initially made a name for itself through attacks on the computer gaming industry. It subsequently branched out into targeting a more diverse range of targets, including organizations in the semiconductor, telecoms, materials manufacturing, pharmaceutical, media and advertising, hospitality, natural resources, fintech, and food sectors.

Blackfly has been closely associated with a second Chinese APT group known as Grayfly, so much so that some vendors track the two groups as one actor: APT41. A 2020 indictment of seven men on charges relating to hundreds of cyber attacks carried out by both groups appeared to shed light on this link. Two Chinese nationals were alleged to have worked with both groups. A crossover in personnel may account for the similarities between both groups.

## Undeterred

Despite being the subject of a U.S. indictment, Blackfly has continued to mount attacks, seemingly undeterred by the publicity afforded to the group. Although it originally made a name for itself by attacking the gaming sector, the group appears focused on targeting intellectual property in a variety of sectors at present.

## 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.

cf6bcd3a62720f0e26e1880fe7ac9ca6c62f7f05f1f68b8fe59a4eb47377880a – Backdoor.Winnkit

e1e0b887b68307ed192d393e886d8b982e4a2fd232ee13c2f20cd05f91358596 – Backdoor.Winnkit

a3078d0c4c564f5efb1460e7d341981282f637d38048501221125756bc740aac – Backdoor.Winnkit

714cef77c92b1d90997258 0ec7602b0914f30e32c09a5e8cb9cb4d32aa2a2196 – Backdoor.Winnkit

192ef0dee8df73eec9ee617abe4b0104799f9543a22a41e28d4d44c3ad713284 – Backdoor.Winnkit

caba1085791d13172b1bb5aca25616010349ecce17564a00cb1d89c7158d6459 – Backdoor.Winnkit

452d08d420a8d564ff5df6f6a91521887f8b9141d96c77a423ac7fc9c28e07e4 – Screenshotting tool

1cc838896fbaf7c1996198309fbf273c058b796cd2ac1ba7a46bee6df606900e – Process-hollowing tool

4ae2cb9454077300151e701e6ac4e4d26dc72227135651e02437902ac05aa80d – SQL tool

560ea79a96dc4f459e96df379b00b59828639b02bd7a7a9964b06d04cb43a35a – Mimikatz

b28456a0252f4cd308dfb84eeaa14b713d86ba30c4b9ca8d87ba3e592fd27f1c – Mimikatz

a3acb9f79647f813671c1a21097a51836b0b95397ebc9cd178bc806e1773c864 – ForkPlayground

5e51bdf067e5781d2868d97e7608187d2fec423856dbc883c6f81a9746e99b9f – Proxy configuration tool

d4e1f09cb7b9b03b4779c87f2a10d379f1dd010a9686d221c3a9f45bda5655ee – Proxy configuration tool

f138d785d494b8ff12d4a57db94958131f61c76d5d2c4d387b343a213b29d18f – Proxy configuration tool

88113bebc49d40c0aa1f1f0b10a7e6e71e4ed3ae595362451bd9dcebcf7f8bf4 – Proxy configuration tool

498e8d231f97c037909662764397e02f67d0ee16b4f6744cf923f4de3b522bc1 – Proxy configuration tool

100cad54c1f54126b9d37eb8c9e426cb609fc0eda0e9a241c2c9fd5a3a01ad6c – Credential-dumping tool