Hive Pro

Threat Level

Amber

THREAT ADVISORY

ATTACK REPORT

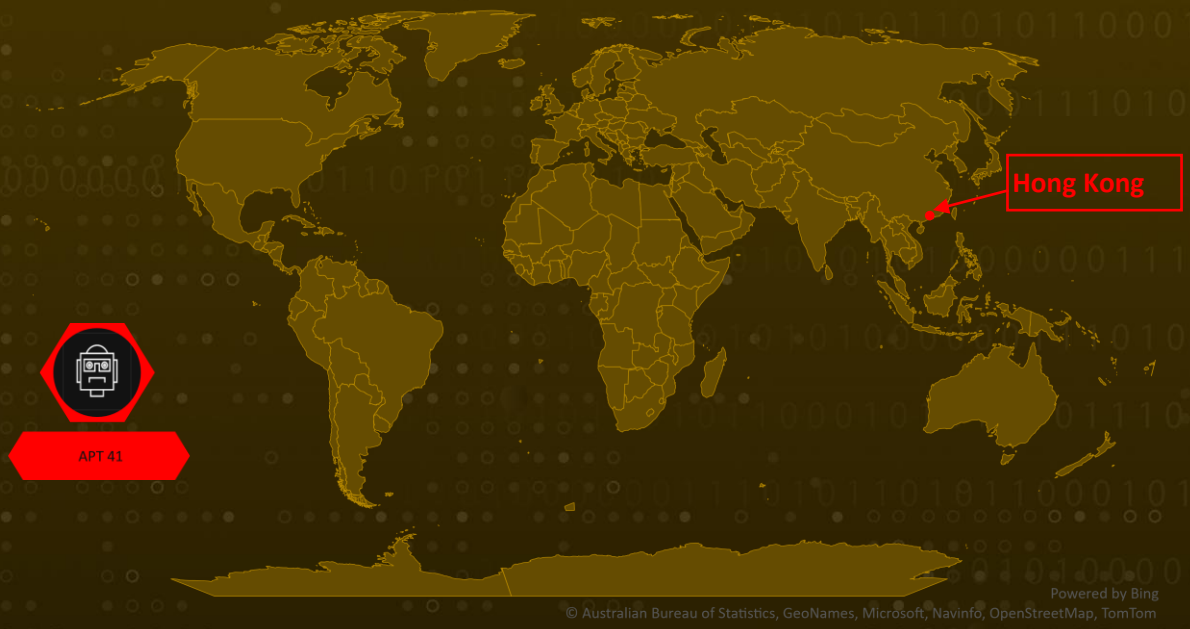
The Spyder Loader malware targets organizations in Hong Kong

Date of Publication	Admiralty Code	TA Number
October 18, 2022	A1	TA2022229

Summary

The Spyder Loader malware was first publicly documented in March 2021. The recent Spyder Loader malware campaign appears to have had the ultimate goal of information theft, and the threat actor behind the campaign could be linked to the China-affiliated espionage group APT41 (a.k.a. Winnti).

Attack Map



Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	**T1591** Gather Victim Org Information	**TA0042** Resource Development	**T1584** Compromise Infrastructure
TA0005 Defense Evasion	**T1055** Process Injection	**TA0008** Lateral Movement	**TA0006** Credential Access
T1003 OS Credential Dumping	**TA0009** Collection	**T1213** Data from Information Repositories	**TA0011** Command and Control
T1105 Ingress Tool Transfer	**TA0010** Exfiltration	**T1041** Exfiltration Over C2 Channel	

Technical Details

#1

Spyder Loader is packaged as a 64-bit Portable Executable (PE) DLL in the recent intrusion. During the initial infection stage, Spyder Loader loads AES-encrypted blobs that create the next-stage payload, "wlbsctrl.dll."

#2

In addition, the malware cleans up accumulated artifacts by overwriting the content of the dumped wlbsctrl.dll file before deleting it. Other post-exploitation tools, such as Mimikatz and a trojanized ZLib DLL module, were also deployed with Spyder Loader.

Indicator of Compromise (IOC)

TYPE	VALUE
SHA-256	00634e46b14ba42c12e35a367f1c7a616fb8e8754ebb2e24ae936377a3ee544a,033313b31fbea64a1a0a53b38c74236f7af2e49018faa2be6c036427c456ef6d,06ed28c4ae295dec0bd692cd7fcecb5fa9de644968d281f5e4bf48eb72bc4b63,091e3e806b6d66cf1eccbd57a787eec65df5f07ad88118c576b3ae06c08af744,0cdbde55b23b26efd5c4503473bd673e3e5a75eae375bae866b6541edb8fcc84,181a25cbcd050c1b42839a5d32df4f59055e27377e71eaa3eb9230a43667f075,228784cc7dad998f1f8b7395bf758827eff9b27762a7056d9e8832bb8a029aad,260d54c2fcf725a8b6d030c36ca26f65ba3d01f707fa0e841cac0166d06218c0,2879253c8c8dd3ee53525c81801d813594bb657ad4f7478ba4288112f0315c9e,2da683d54f12d83f0f111b5c57f7f78016cad5860b2604d38b2aba37ab3d5c55,3196e74004816227323d6864448361fb173b3c96cf3d1b0aa26dfcd259a61505,33aa5df5470ae59cd30c7ea4c2ad1e13901a8fd13ea6b4b5584d10ffdba31ee4,396e35b2a4f920182d3148c834cf70f00b6094600e51e030d6fc297cb0ca5c06,3b3df3ada05e521ec8ce2f0deaeb6fd4359a2de9cadb0dd51c0d9d7a8354

References

https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/spyder-loader-cuckoobees-hong-kong

What Next?

Book a free demo with **HivePro Uni5** to check your exposure to this advisory. HivePro Uni5 is a Continuous Threat Exposure Management Solution that proactively reduces an organization's attack surface before it gets exploited.

At Hive Pro we take a long hard look at your vulnerabilities so you can bolster your defenses and fine-tune your offensive cybersecurity tactics.

REPORT GENERATED ON

October 18, 2022 . 5:55 AM

More at www.hivepro.com