Hive Pro

Threat Level

Red

THREAT ADVISORY

ACTOR REPORT

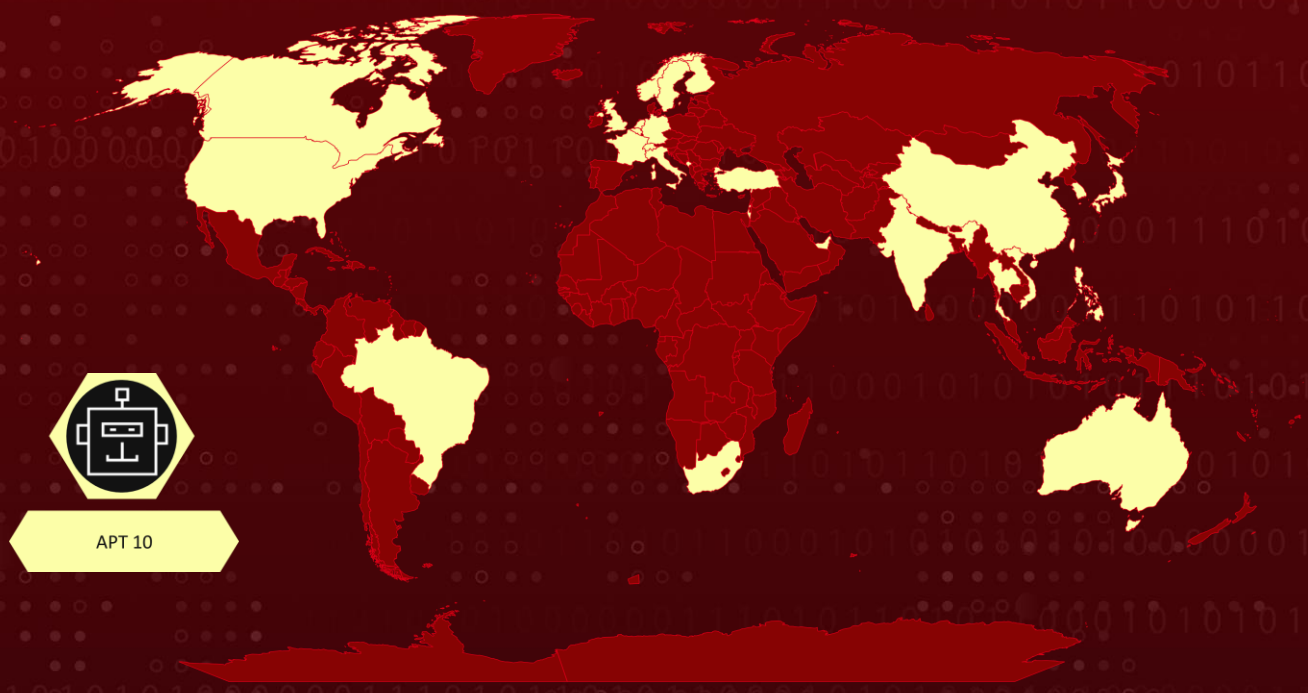
APT10 distributes LODEINFO malware to deploy infection chains

Date of Publication	Admiralty code	TA Number
November 2, 2022	A1	TA2022242

Summary

The APT 10 cyber espionage gang has been spotted adopting a new stealthy infection chain to deploy the LODEINFO backdoor shellcode to exfiltrate sensitive information to Command and Control (C2).

Actor Map



Potential MITRE ATT&CK TTPs

TA0002 Execution	**TA0005** Defense Evasion	**TA0007** Discovery	**T1059** Command and Scripting Interpreter
T1027 Obfuscated Files or Information	**T1140** Deobfuscate/Decode Files or Information	**T1124** System Time Discovery	**T1082** System Information Discovery

Technical Details

#1 During the initial phase of the attack, a spear-phishing email with a malicious attachment was delivered to install malware persistence modules, which consisted of a valid EXE file and a malicious DLL file loaded via the DLL sideloading technique.

#2 The malicious DLL file contains a LODEINFO shellcode loader. Another form of infection employs a self-extracting archive (SFX) file in RAR format, which comprises three files containing self-extracting script commands. It has been noticed in several incidents that the infection vector used a file-less downloader shellcode called "DOWNIISSA".

#3 After infiltrating the target machine, the LODEINFO backdoor transfers machine information to the C2. Furthermore, junk data is appended at random to the end of the data, potentially to avoid detection based on packet size.

Actor Detail

<table>
<tr><th>NAME</th><th>ORIGIN</th><th>TARGET COUNTRIES</th><th>TARGET INDUSTRIES</th></tr>
<tr><td rowspan="3">APT 10(Stone Panda, menuPass Team, menuPass,Red Apollo,CVNX, Potassium, Hogfish, Happyyongzi, Cicada, Bronze Riverside, CTG-5938,ATK 41,TA429,ITG01)</td><td>China</td><td rowspan="3">Australia, Belgium, Brazil, Canada, China, Finland, France, Germany, Hong Kong, India, Israel, Italy, Japan, Montenegro, Netherlands, Norway, Philippines, Singapore, South Africa, South Korea, Sweden, Switzerland, Taiwan, Thailand, Turkey, UAE, UK, USA, Vietnam.</td><td rowspan="3">Aerospace, Defense, Energy, Financial, Government, Healthcare, High-Tech, IT, Media, NGOs, Pharmaceutical, Telecommunications, Think- Tanks, Biomedical , Consulting , Manufacturing , Oil and Gas ,</td></tr>
<tr><td>MOTIVE</td></tr>
<tr><td>Information theft and espionage</td></tr>
</table>

Indicator of Compromise (IOC)

TYPE	VALUE
MD5	da20ff8988198063b56680833c298113,89bd9cf51f8e01bc3b6ec025ed5775fc,,cb2fcd4fd44a7b98af37c6542b198f8d,a0828f194d3835ea218609dd93d87d16,16cd587529c230b1a6b47b66d3c84fcf,de4c87a05becc78ab2e3f568cd46272c,9066bec5834279ffcb8876f2fdb8752c,016a974e70bbce6161862e0ac01a0211,d3cae3b6d948ffd17c5a165bad94f857,16f0b02bf9676d066d245fe0c717ba52,ff71fadc33b883de934e632ddb4c6b78,1a5a74453ebb9747b433342d1ba242cc,013ef386b1c792faec51fc550fef063a,da1c9006b493d7e95db4d354c5f0e99f,a8220a76c2fe3f505a7561c3adba5d4a,26892038ab19c44ba55c84b20083cdbd,c5bdf14982543b71fb419df3b43fbf07,db0bfce29c7c2f076f711cdde2898227,a809231cf901bad9d643494d0eb5a630,0fcf90fe2f5165286814ab858d6d4f2a,ad206315afaa0cd5b42f0fc7b537fefd,c9d724c2c5ae9653045396deaf7e3417,f7de43a56bbb271f045851b77656d6bd,15b80c5e86b8fd08440fe1a9ca9706c9,6780d9241ad4d8de6e78d936fbf5a922,76cdb7fe189845a0bc243969dba4e7a3,edc27b958c36b3af5ebc3f775ce0bcc7
IPV4	103.175.16[.]39 172.104.72[.]4 172.104.112[.]218 172.105.223[.]216 202.182.108[.]127 45.77.28[.]124 5.8.95[.]174
Domain	www.dvdsesso[.]com

References

https://securelist.com/apt10-tracking-down-lodeinfo-2022-part-i/107742/

https://securelist.com/apt10-tracking-down-lodeinfo-2022-part-ii/107745/

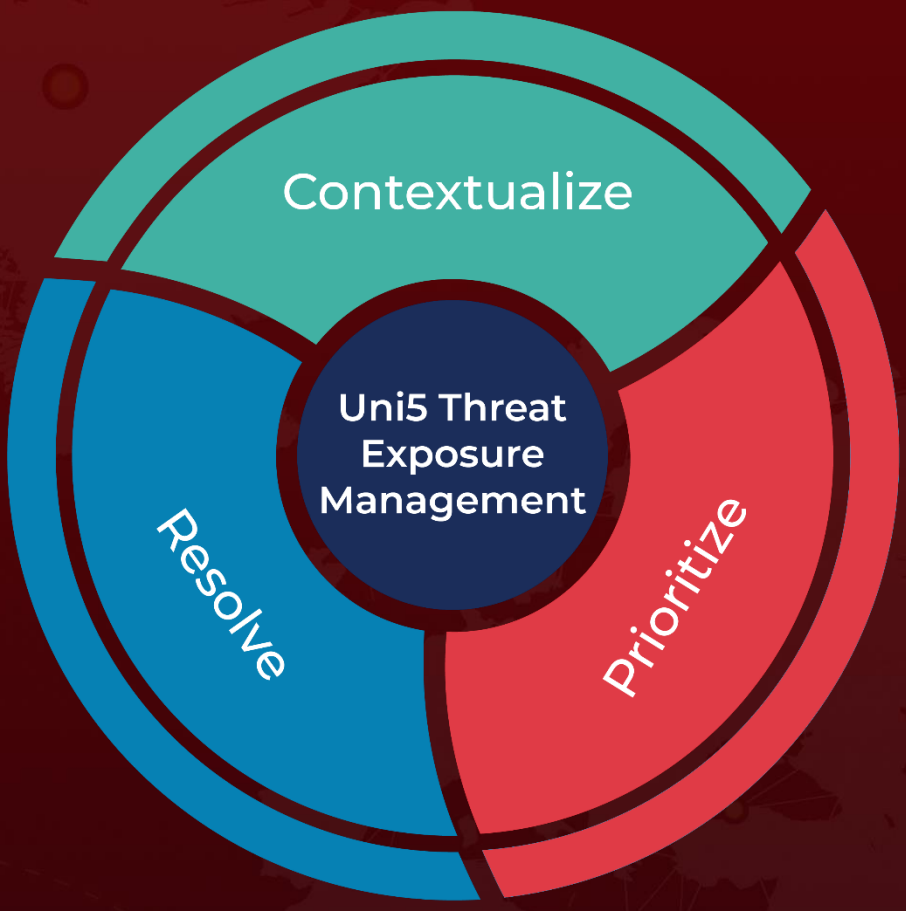
https://thehackernews.com/2022/11/chinese-hackers-using-new-stealthy.html

https://attack.mitre.org/groups/G0045/

What Next?

At **HivePro**, 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 **Hive Pro Uni5**: Continuous Threat Exposure Management Platform.



REPORT GENERATED ON

November 2, 2022 • 4:55 AM

More at www.hivepro.com