Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

ChamelGang's Double Play: Strategy Beyond Encryption

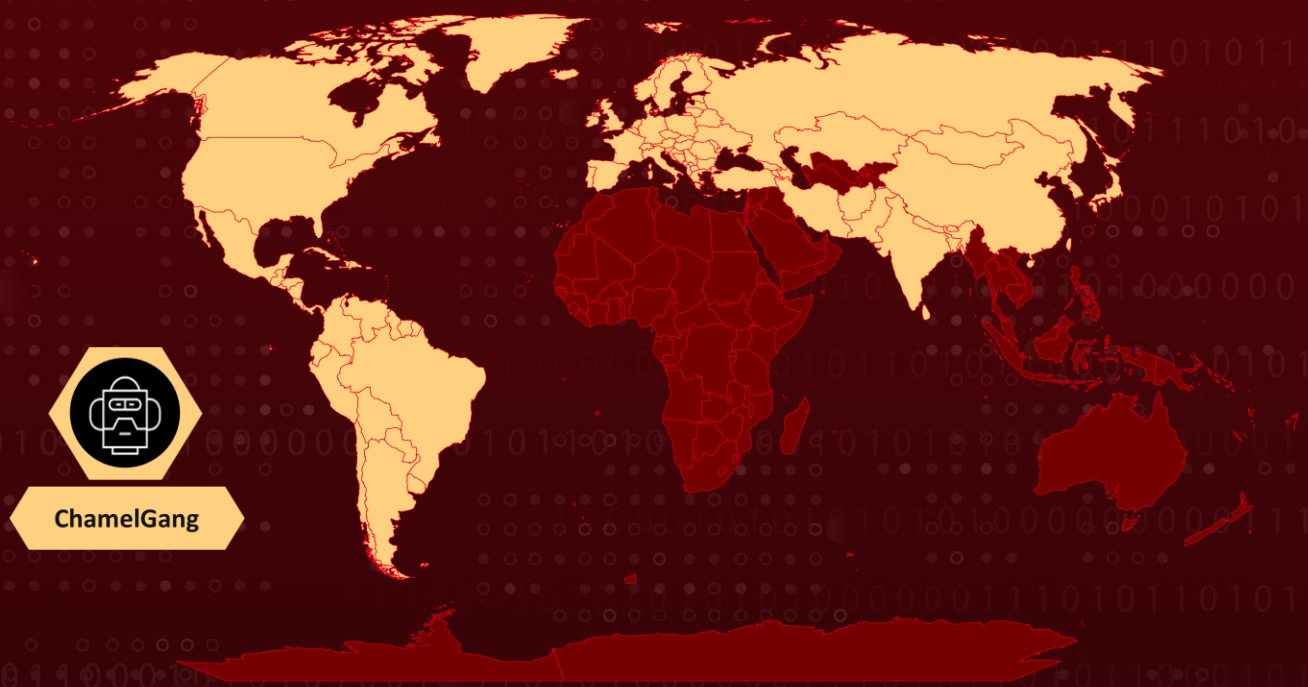
Date of Publication	Admiralty Code	TA Number
June 27, 2024	A1	TA2024248

Summary

Active Since: 2021
Threat Actor: ChamelGang (aka CamoFei)
Malware: CatB Ransomware
Attack Regions: East Asia, South Asia, North America, South America, and Europe
Targeted Industries: Aviation, Business Services, Construction, Consulting, Critical Infrastructure, Education, Finance, Food, Gambling, Government, Healthcare, Legal, Manufacturing, Media, Non-Profit, Research, Retail, Software, Textiles

Attack: ChamelGang, also known as CamoFei, represents a prominent cyberespionage entity renowned for deploying ransomware to obscure attack origins, deflect defensive measures, and secure additional financial rewards while engaging in data theft. This threat actor linked to China has been active since at least 2021, targeting victims across numerous countries.

Attack Regions



Attack Details

#1 ChamelGang, also known as CamoFei, is a Chinese cyberespionage group that employs ransomware tactics to complicate attack attribution, divert defenders, and achieve secondary financial gains alongside data theft.

#2 A distinct activity cluster within this group leverages intrusions using off-the-shelf tools like BestCrypt and BitLocker. These attacks have impacted various industries across North America, South America, and Europe, with a particular focus on the US manufacturing sector, government, and critical infrastructure. Although attribution remains ambiguous, the objectives appear consistent.

#3 ChamelGang's cyberespionage operations disguised as ransomware attacks offer adversarial nations plausible deniability, as the actions can be attributed to independent cybercriminal actors rather than state-sponsored entities. This strategic use of ransomware serves purposes of financial gain, disruption, and misattribution.

#4 ChamelGang has also targeted a government organization in East Asia and critical infrastructure sectors, including an aviation organization in the Indian subcontinent. The group employs sophisticated techniques for initial access, reconnaissance, lateral movement, and data exfiltration.

#5 In the final stage of their attacks, ChamelGang deploys CatB ransomware on the network, leaving ransom notes at the beginning of each encrypted file. Observed activities include the use of publicly available tools and their custom malware, BeaconLoader. They provide a ProtonMail address for contact and a Bitcoin address for payment.

Recommendations

Network Segmentation: Utilize network segmentation to isolate critical infrastructure and sensitive data from less secure parts of the network. This can help contain the spread of ransomware and limit access to valuable assets in case of a breach.

Secure Configuration Management: Enforce secure configurations for all systems and applications based on industry standards and vendor recommendations. This reduces the attack surface and minimizes vulnerabilities that could be exploited by cyberespionage groups.

Endpoint Hardening: Harden endpoints by disabling unnecessary services and features, applying least privilege principles to user accounts, and configuring firewalls and host-based intrusion prevention systems (HIPS) to block unauthorized access attempts.

Secure Remote Access: Secure remote access solutions using strong authentication methods, such as VPN with MFA, and limit administrative access to critical systems. Monitor remote access logs for unusual login patterns or unauthorized access attempts.

Data Backups: Implement frequent backups for all assets to ensure their complete safety. Implement the 3-2-1-1 backup structure and use specialized tools to provide backup resilience and accessibility.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0003** Persistence	**TA0005** Defense Evasion	**TA0006** Credential Access
TA0007 Discovery	**TA0009** Collection	**TA0011** Command and Control	**TA0010** Exfiltration
TA0040 Impact	**T1190** Exploit Public-Facing Application	**T1133** External Remote Services	**T1003** OS Credential Dumping
T1016 System Network Configuration Discovery	**T1068** Exploitation for Privilege Escalation	**T1046** Network Service Discovery	**T1057** Process Discovery
T1033 System Owner/User Discovery	**T1027** Obfuscated Files or Information	**T1083** File and Directory Discovery	**T1105** Ingress Tool Transfer
T1082 System Information Discovery	**T1482** Domain Trust Discovery	**T1078** Valid Accounts	**T1018** Remote System Discovery

T1069.002 Domain Groups	**T1560.001** Archive via Utility	**T1136.002** Domain Account	**T1069.001** Local Groups
T1219 Remote Access Software	**T1657** Financial Theft	**T1490** Inhibit System Recovery	**T1562.001** Disable or Modify Tools
T1486 Data Encrypted for Impact	**T1041** Exfiltration Over C2 Channel		

Indicators of Compromise (IOCs)

TYPE	VALUE
Bitcoin Address	bc1qakuel0s4nyge9rxjylsqdxnn9nvyhc2z6k27gz
Domain	resources.albaclass[.]com
IPv4	185[.]225[.]19[.]61
URL	hxxp[:]//185[.]225[.]19[.]61[:]80/3[.]txt
SHA1	098e60cd5053ec9613d32a7ced68e44f1a417353, 09959be9b5f8ca21caa55577ce620034632a3f92, 0c762bff5b4a0bf5abbdf28afc15cfc6dce575b1, 15b0a25b4e55241b12d09633465d3109c324fb98, 19114f25a5681149ae3950fb0c52d59a69d031dc, 1e12b053a643895e071be3538bb9950667134563, 1fa6de645e7146a0a1b64e17d260546e598acd17, 24eb404a8daaace36a2cf5fb0f7b8608d2a3963a, 33009aaea3d58d8f72dfaf45dd8016707599d6c0, 374882c4752a05ec52e41943d7e3de8c1cccef10, 398c4c0ba6f5ea78175dd2846067f10d3864a2cc, 44759a6597bad3a287a7b82724a763208c599135, 57373d25527b3adf54eefcbfb69b41a513605af0, 5c15b0ad93f2a4ae08a2a8e070afb99795855e0f, 5d43ee1f75781033cd5accf298583529bdd12fa1, 608c2a64c9d41b891c18cb682a01eabf035a7f50, 65867d738ee978811a098a766810726e39d1391e, 782b157e901326d67a783e3e7dac9694a87dc7c2, 8052fcd408d9bd9e7594accdabb161ba8c4a9bd7, 882efb1b8093c46223e71e2be353b6a95dc24e7a, 8ce96c0eb64db6856908fde2a1e9bcc387ce2744,

TYPE	VALUE
SHA1	8e76a2cc57fa5390462839c0471f522db3882c66, 951e603af10ec366ef0f258bf8d912efedbb5a4b, 9d1076b58f30142fe1c693b4edcec9816b3cb3c6, a2a81d5fcc0012e78fe4fe1b681a82c3158ce2bf, a566e410144d5972a92dc21de37e2b8617bfc347, a566e410144d5972a92dc21de37e2b8617bfc347, a79bc5e91761c98d99dc028401cd284c3b340474, bd22ce42492bdad203ce1c712e075d422f70bbd3, c1eb7d5b772635d519cb6f4f575ada709d626c1a, d4828b63b596cf8d069b97a8a9396928ec3ad216, db99fc79a64873bef25998681392ac9be2c1c99c, dcd3f2a8ec1e63cb1bfcaa622ae48373ce0a01ce, de8bf4153bd72ef668b9a60419794ccabbe87c4f, dfab55758b195d1d30d89ba9175da3a49dc180be, e7ee9c41a1137b50d81238ae35b927f6ebbaae83, efa16441d95984bb5b278aa510e9942a40356f84, f4529b672eec3f629184fa4c62c3743ae5354f95

References

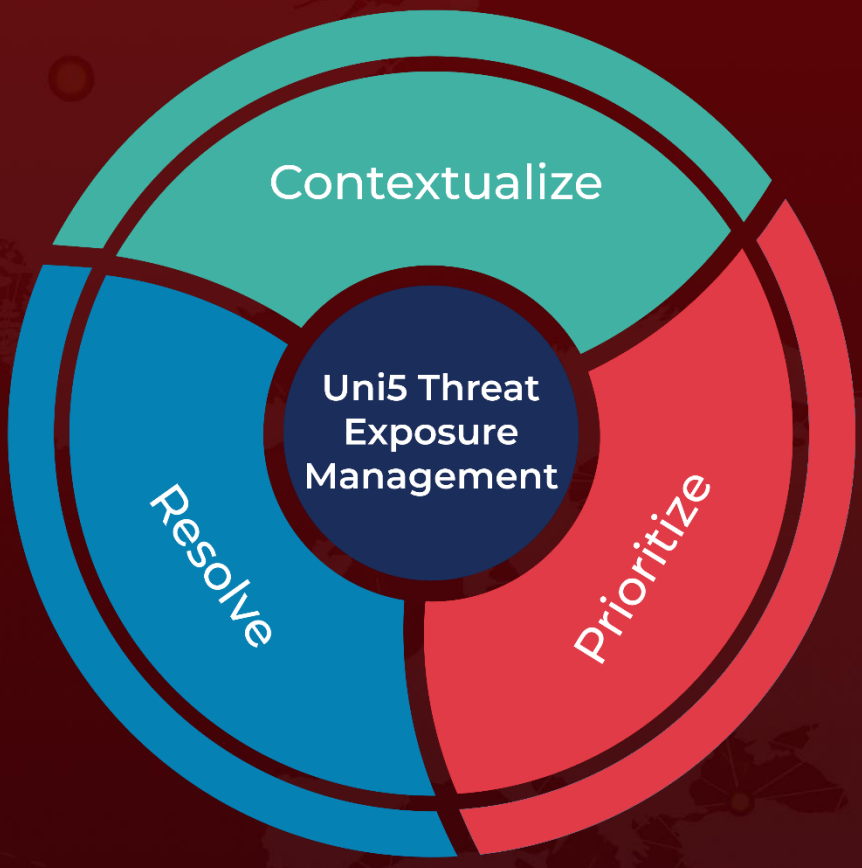
https://assets.sentinelone.com/sentinellabs/chamelgang-friends-en

https://www.hivepro.com/threat-advisory/chamelgang-strikes-again-with-chameldoh-malware-xdns-over-https/

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

June 27, 2024 • 10:30 PM

More at www.hivepro.com