THREAT CURE
RE-ARCHITECT YOUR THREAT LANDSCAPE

ThreatCure

Cyber Threat Advisory

CHRYSENE

Threat Actor Criminal

Description

CHRYSENE

CATEGORY

Criminal

SEVERITY

High

Platforms

Windows

IMPACT

- Operational Disruption
- Data Breaches and Espionage
- Financial Losses

CHRYSENE, a threat group believed to have ties with the Iranian government, has recently extended its operations to Pakistan in addition to its traditional focus on the Middle East. This group is known for targeting key sectors like energy, finance, and government through long-term intelligence-gathering campaigns. They leverage social engineering techniques, phishing emails, and customized malware such as SHAPESHIFT and MARCO to infiltrate networks. Their tactics also include the use of PowerShell scripts for lateral movement and exploiting supply chain relationships to compromise primary targets. Recently, CHRYSENE has increased its use of cloud-based infrastructure for command-and-control activities and refined its strategies to bypass multi-factor authentication through sophisticated social engineering.

Over time, CHRYSENE has been identified under various aliases by cybersecurity researchers, highlighting its adaptability and diverse threat operations. These aliases include Cobalt Gypsy, Ballistic Bobcat, Educated Manticore, Timberworm, ATK 40, Magic Hound, CharmingCypress, Twisted Kitten, APT 34, Rocket Kitten, Storm-0861, Yellow Maero, Group 26, Tarh Andishan, Evasive Serpens, NewsBeef, Mint Sandstorm, Ajax Security Team, UNC788, Cobalt Mirage, Flying Kitten, TunnelVision, UNC1860, Yellow Garuda, EUROPIUM, Hazel Sandstorm, TA452, Cobalt Illusion, Crambus, TA453, APT 35, Phosphorus, ITG13, TG-2889, Group 83, OilRig, IRN2, Charming Kitten, Helix Kitten, TEMP.Beanie, Earth Simnavaz, DEV-0861, Scarred Manticore, Parastoo, Newscaster, and Cutting Kitten. These numerous identities reflect the group's complex operations and the wide scope of its global activities.

Kill Chain

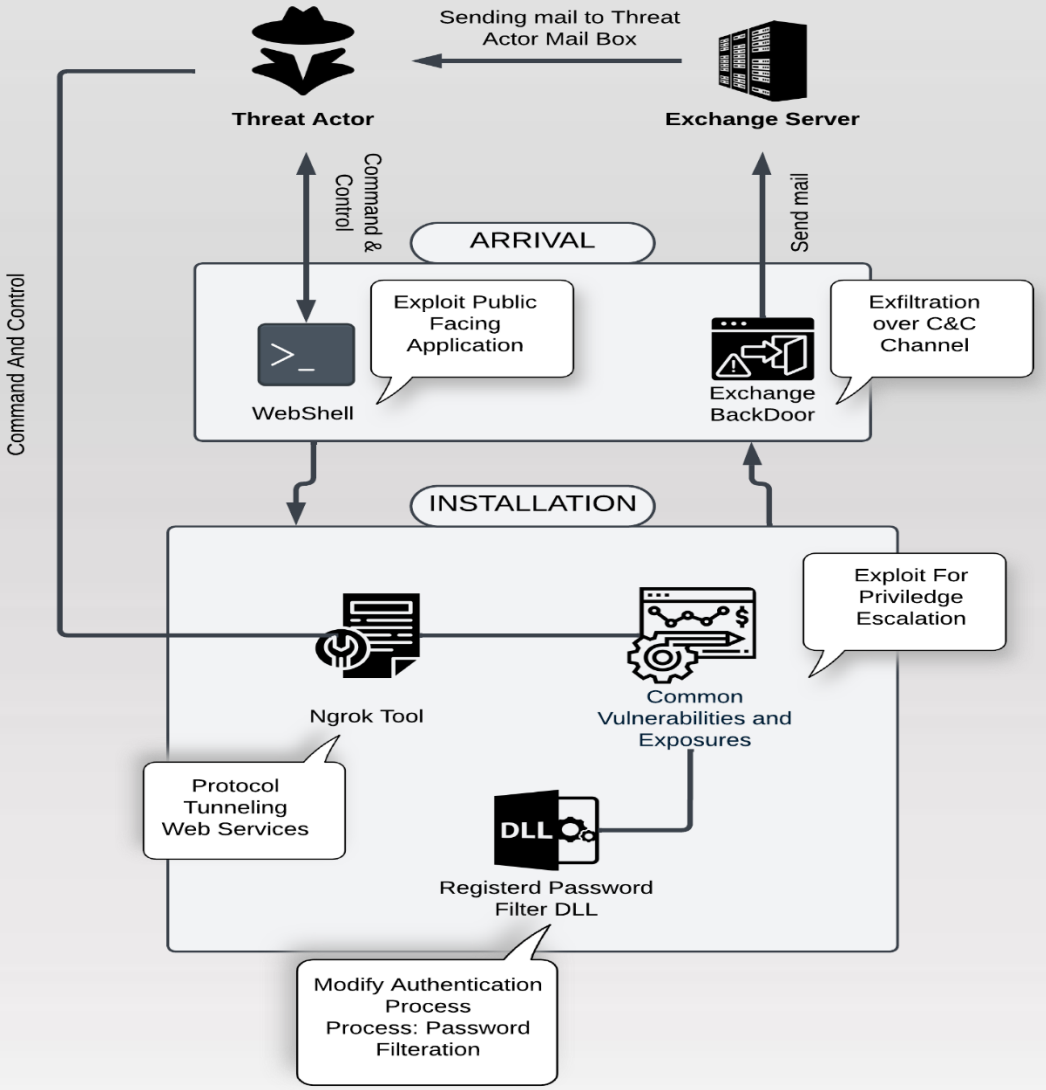

Figure 1 Kill Chain

Indicator of Compromise

SHA256

a24303234e0cc6f403fca8943e7170c90b69976015b6a84d64a9667810023ed7
bf308e5c91bcd04473126de716e3e668cac6cb1ac9c301132d61845a6d4cb362
88097e4780bfdc184b16c5a8a90793983676ad43749ffca49c9d70780e32c33a
918e70e3f5fdafad28effd512b2f2d21c86cb3d3f14ec14f7ff9e7f0760fd760
d6048c65e0dae602043c1d4b86477996cde46d084c30cb28723b93a2ff40fe4a
54e8fbae0aa7a279aaedb6d8eec0f95971397fea7fcee6c143772c8ee6e6b498
b3257f0c0ef298363f89c7a61ab27a706e9e308c22f1820dc4f02dfa0f68d897
98fb12a9625d600535df342551d30b27ed216fed14d9c6f63e8bf677cb730301
edfae1a69522f87b12c6dac3225d930e4848832e3c551ee1e7d31736bf4525ef
0b99db286f3708fedf7e2bb8f24df1af13811fe46b017b6c3e7e002852479430
c22d25107e48962b162c935a712240c0a4486b38891855f0e53d5eb972406782
dfb3e5f557a17c8cdebdb5b371cf38c5a7ab491b2aeaad6b4e76459a05b44f28
c3a29c2457f33e54298a1c72a967aa161a96b0ae62ffbefe9e5e1c2057d7f3f4
a9c92b29ee05c1522715c7a2f9c543740b60e36373cb47b5620b1f3d8ad96bfa
9793ea98b7fbd43f0a7273594d7b4e53338048c651c33fbfdbeb1cc275957996
e733b9444106ca37c3ef9e207ac6c813b787614496b275c1a455fccc3aca1c4a
3ab29bc71ddd272f33f17c5108c044a570610c06ccba16cde1a4aa67b1524a8b
42acdf5051bc636dbbb56483fbca925238f1c5422497e2dda73f07b0653e56f2

Indicator of Compromise

MD5

5b974268236aafd6dc7151758e508069
bb4c8f42cc624c628e4b98bd43f29fa6
3528837b4088a22f0043551431809b3d
f9914c7d6e09d227b2cecea50b87e58b
8f2ba0fd8059253728812c7a15285dbb
ee59031802287179d0abaac41fb34a66
73690743aea09a345dbdfe828f069370
60adbb2a2aa829c0ef7bbfce5214ff82
db89ec570e6281934a5c5fcf7f4c8967
082bb47f808e5e650cf94c50aa13658a
1062db7b804ae39995ffde695275ac0c
2e6808a4d0c8cfd1d9a347f8cf80dc6d
6a159081da3a84e50571202655b4cf10
8afdfd6d035b3c616dc37894a15206b4
79cc8730d748a884cc666b95ee9fed36
58e67cdc9ef57805f45ba554bdccb3b1
a79e4424116dc0a76a179507ac914578
d56b5fd6b8976c91d2537d155926afff

Remediation

1. **Patch Management:** Regularly update and secure systems to address vulnerabilities commonly exploited by CHRYSENE.
2. **Email Security:** Strengthen defenses against spear-phishing attempts by deploying advanced filtering solutions.
3. **Network Monitoring:** Monitor network traffic for unusual DNS tunneling and HTTP patterns linked to CHRYSENE activity.
4. **Endpoint Protection:** Utilize behavior-based detection tools to identify and block malicious operations.
5. **Access Control:** Apply least privilege principles and enforce multi-factor authentication to protect sensitive data.
6. **Incident Response:** Develop and test a response plan to quickly detect, contain, and address CHRYSENE's attacks.
7. **Threat Intelligence:** Stay updated on CHRYSENE's evolving techniques to proactively adapt defenses.
8. **Employee Training:** Educate employees on phishing tactics and the importance of recognizing suspicious activity.

ThreatCure

Cyber Threat Advisory

Secure your byte world

CHRYSENE

Threat Actor Criminal

Get Started Today

For more information about the ThreatCure ShieldOps Platform
or to schedule a demo, please contact:

- Website: www.threatcure.net
- Email: info@threatcure.net

THREAT CURE
RE-ARCHITECT YOUR THREAT LANDSCAPE