Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

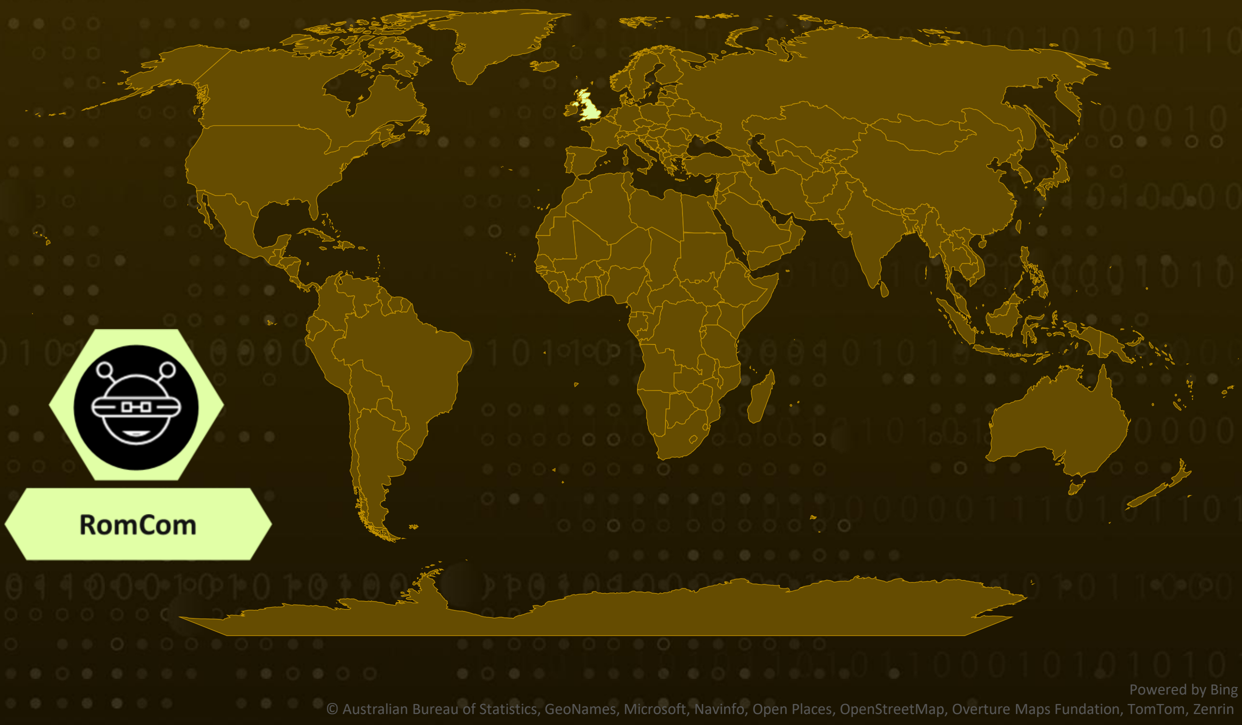
Operation Deceptive Prospect: RomCom's New Social Engineering Playbook

Date of Publication	Admiralty Code	TA Number
May 6, 2025	A1	TA2025136

Summary

Attack Discovered: March 2025
Targeted Countries: UK
Affected Industries: Retail, Hospitality, and CNI (Critical National Infrastructure) sectors
Actor: RomCom (aka Storm-0978, Tropical Scorpius, Void Rabisu, DEV-0978, UNC2596, UAC-0180)
Campaign: Operation Deceptive Prospect
Attack: In a malicious campaign dubbed Operation Deceptive Prospect, the RomCom threat group disguised malicious emails as fake customer complaints to trick UK based services into clicking phishing links. By using realistic personas and impersonating platforms like Google Drive, they aimed to quietly drop malware disguised as documents. Their evolving tactics clever social engineering, abuse of trusted cloud services, and spoofed domains highlight a growing threat that blends technical skill with human manipulation.

Attack Regions


RomCom
Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, Overture Maps Fundation, TomTom, Zenrin

Attack Details

#1 In March 2025, a phishing campaign dubbed "Operation Deceptive Prospect" was uncovered, which closely resembled tactics used by the Russian-linked threat group RomCom. This campaign specifically targeted customer service teams at UK based organizations in the retail, hospitality, and critical national infrastructure sectors.

#2 RomCom has been active since 2022. Over time, the group has evolved into a more refined cyber-espionage and cybercrime entity, known for using spear-phishing campaigns and weaponized installers of legitimate software. While RomCom's early motives included financial gain through ransomware and extortion, more recent campaigns show a pivot towards intelligence gathering and credential theft.

#3 The campaign's phishing emails were cleverly crafted using personas that mimicked legitimate English-speaking individuals. They referenced issues such as stolen luggage or poor airport conditions, including fabricated documents like police reports or travel feedback to build credibility. These emails, sent through real feedback portals using Yahoo addresses, followed a formulaic structure designed to exploit the recipient's sense of responsibility.

#4 To maintain stealth and credibility, RomCom leveraged domain registration services and cloud hosting platforms such as Amazon S3. This use of widely trusted services helps the attackers evade detection during the early stages of their attacks. Nearly 100 domains were identified that followed RomCom's usual playbook featuring terms like “drive,” “storage,” and numeric/punctuation tricks to look legitimate. These domains served as delivery points for fake documents that triggered malware downloads once clicked.

#5 Once a user clicked on the malicious link, the attack chain redirected them via a shortened URL to fake cloud storage pages. These were designed to imitate OneDrive download pages and hosted payloads named to look like legitimate PDFs. The backend infrastructure used by RomCom included ASNs like SHOCK-1 and hosting providers.

#6 RomCom's attack infrastructure was further supported by DNS services and file-sharing platforms. Although the exact name of the final payload file remains unknown, forensic analysis on similar samples confirmed strong ties to RomCom's malware family. With a blend of social engineering, impersonation, and infrastructure obfuscation, this campaign illustrates RomCom's evolving strategies and its growing capabilities in both cybercrime and espionage.

Recommendations

Protect Customer-Facing Forms: Make sure any forms on your website like feedback or contact forms are well-protected. Add features like CAPTCHA to stop bots, check for strange or fake inputs, and watch for suspicious activity so attackers can't pretend to be real customers and sneak in harmful links.

Strengthen Email Safety and User Awareness: Use smart email filters to catch phishing emails before they reach your team. At the same time, regularly train customer service staff to spot red flags like urgent messages, unexpected document links, or fake versions of Google Drive or OneDrive so they know what to avoid and how to report it.

Least Privilege: Implement stringent access policies and enforce least privilege principles to prevent unauthorized access and contain the spread of malware within the organization's network.

Enhance Endpoint Protection: Deploy next-generation antivirus (NGAV) and endpoint detection & response (EDR) solutions to identify and block malware. Leverage behavioral analysis and machine learning-based detection to spot suspicious activity.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0005 Defense Evasion
TA0010 Exfiltration	TA0011 Command and Control	T1036 Masquerading	T1036.008 Masquerade File Type
T1199 Trusted Relationship	T1497 Virtualization/Sandbox Evasion	T1553 Subvert Trust Controls	T1553.002 Code Signing
T1566 Phishing	T1566.002 Spearphishing Link	T1583 Acquire Infrastructure	T1584 Compromise Infrastructure

T1584.003 Virtual Private Server	**T1585** Establish Accounts	**T1585.002** Email Accounts	**T1587** Develop Capabilities
T1587.002 Code Signing Certificates	**T1588** Obtain Capabilities	**T1588.007** Artificial Intelligence	**T1656** Impersonation
T1204 User Execution	**T1204.001** Malicious Link	**T1059** Command and Scripting Interpreter	

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	drivepoint[.]pub, drshare[.]online, opn[.]to, cloudly[.]live, 1dcloud[.]live, drivenc[.]pub, onestorelink[.]live, 1day[.]live, 1drv365[.]online, my-drive365[.]pub, 365msdrv[.]live, 1dv365[.]live, my1drv[.]live, data-dv[.]live, ondv[.]live, onedrweb[.]live, 1dv[.]online, sharedrive[.]pub, drivehost[.]live, dvcloud[.]live, cloud1dv[.]com, gcloud-drive[.]com, 1dvstorage[.]com, cloudedrive[.]com, datadrv1[.]com, onelivedrv[.]com
Email Addresses	brain[.]welch381761@yahoo[.]com, kajzer[.]david962701@yahoo[.]com, calvertadam317304@yahoo[.]com

TYPE	VALUE
IPv4	45[.]95[.]18[.]138, 77[.]91[.]76[.]176, 185[.]117[.]91[.]134, 77[.]239[.]101[.]131, 213[.]139[.]205[.]220, 193[.]42[.]39[.]159
SHA256	8b683ed0d1cd0139093e21889be077d0e4e50e7adaf638b56e2077df5c6eda4b, 8183f4b75cbe318a34846b0d8bb9caf219b4b2686d14a531090b6550398cbbca, 4055e3a45d63778dfc5775ae6e512fb3991df1dadf91630a26ed5747e350f75f

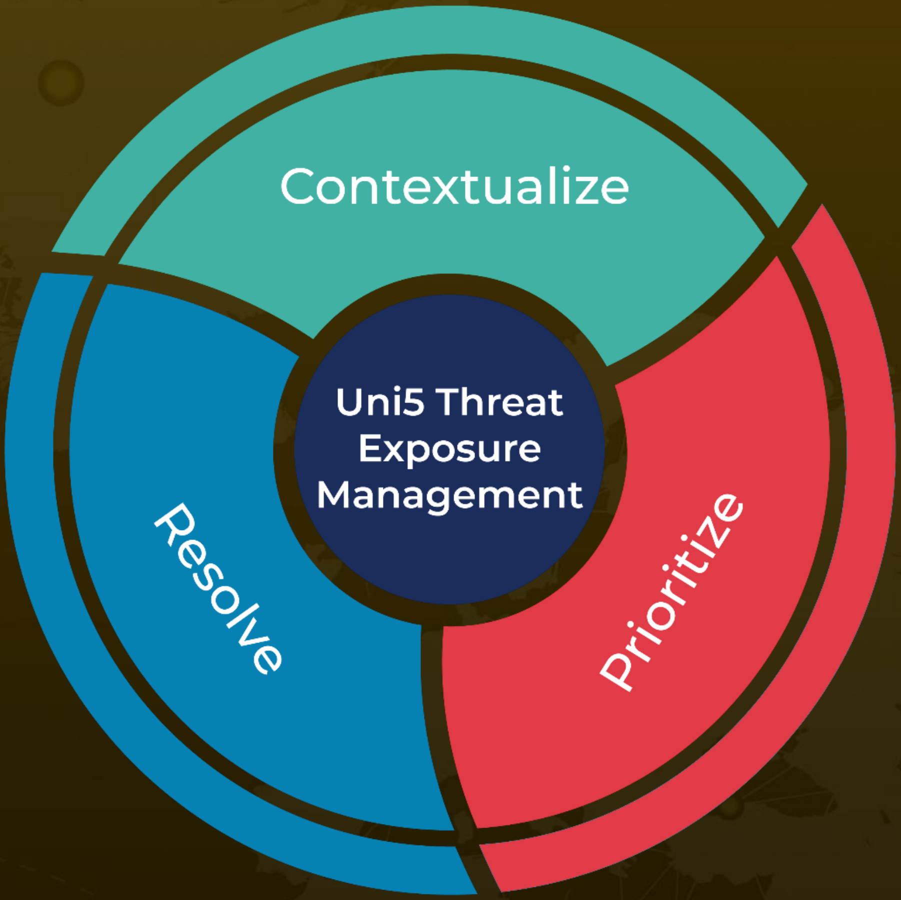
References

https://www.bridewell.com/insights/blogs/detail/operation-deceptive-prospect-romcom-targeting-uk-organisations-through-customer-feedback-portals

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

May 6, 2025 • 5:30 AM

More at www.hivepro.com