Hive Pro®

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

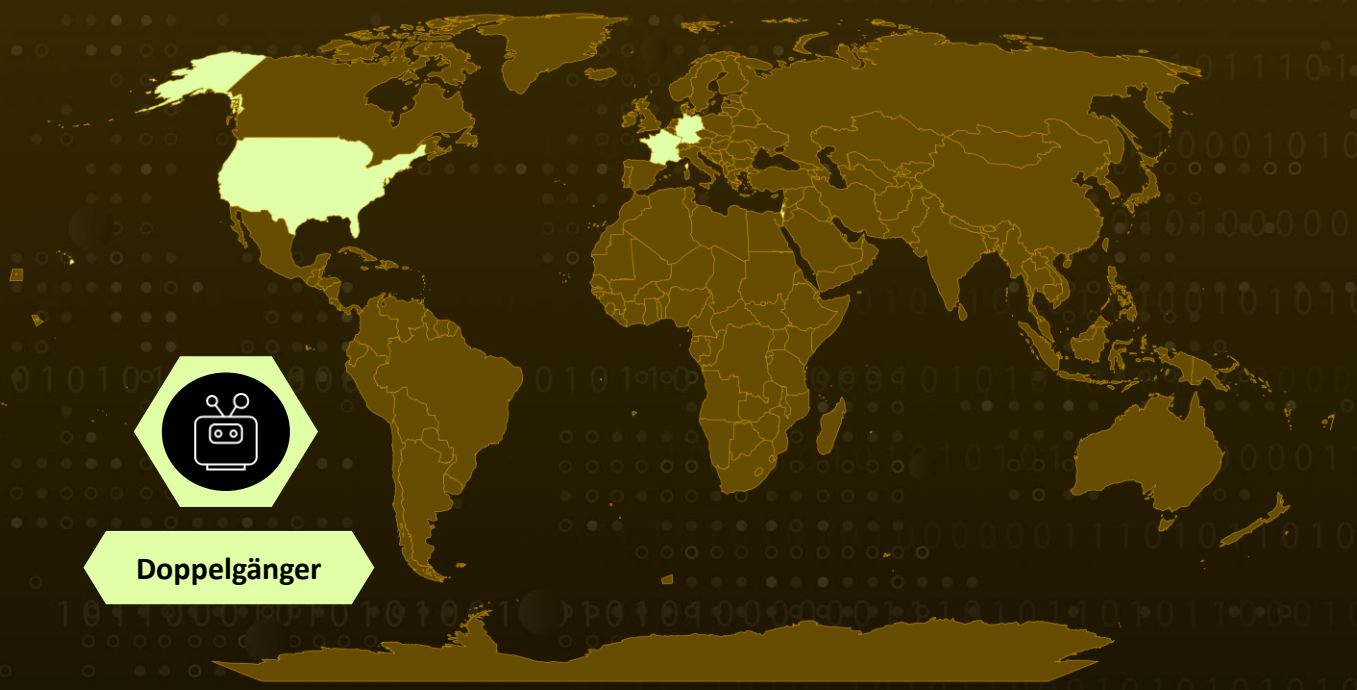
Unmasking Doppelgänger: Russia's Disinformation Campaign Revealed

Date of Publication	Admiralty Code	TA Number
February 27, 2024	A1	TA2024078

Summary

Attack Began: November 2023
Targeted Countries: Germany, the United States, Israel, and France
Threat Actor: Doppelgänger
Targeted Industries: Government, Media
Attack: Doppelgänger, a suspected Russia-aligned influence operation network targeting German audiences with propaganda and disinformation, potentially aiming to sway opinions ahead of elections. Doppelgänger employs coordinated social media activities and a dynamic infrastructure to maximize its impact and evade detection.

Attack Regions



Attack Details

#1 An influence operation network named Doppelgänger, suspected to be Russia-aligned. The network has been intensively targeting German audiences with propaganda and disinformation, particularly criticizing the ruling government coalition and its support for Ukraine, potentially aiming to influence public opinion ahead of upcoming elections.

#2 Doppelgänger operates a substantial network of social media accounts, coordinating activities to maximize visibility and engagement. The network utilizes a multi-stage approach to disseminate content, employing obfuscation and tracking techniques.

#3 Additionally, Doppelgänger creates and manages websites hosting articles tailored to German audiences, often with anti-government narratives. The infrastructure supporting Doppelgänger's activities is dynamic, with domains frequently changing and servers implementing geofencing. Despite efforts to counter influence operations, continued vigilance and collaboration are required to mitigate their impact effectively.

Recommendations

Enhancing Public Awareness and Media Literacy: Educating the public about the tactics used in influence operations can help individuals identify and resist manipulation. Media literacy programs can teach critical thinking skills to discern credible information sources from propaganda and disinformation.

Monitoring and Detection: Implementing robust monitoring systems to detect suspicious activities on social media platforms and other online channels can help identify and mitigate the spread of propaganda and disinformation.

Transparency and Accountability: Social media platforms should prioritize transparency in their algorithms and policies, disclosing information about how content is recommended and promoted. Platforms should also hold users accountable for spreading false information or engaging in coordinated manipulation.

Potential MITRE ATT&CK TTPs

TA0003 Persistence	TA0002 Execution	TA0040 Impact	TA0005 Defense Evasion
TA0011 Command and Control	TA0043 Reconnaissance	TA0042 Resource Development	T1140 Deobfuscate/Decode Files or Information
T1593 Search Open Websites/Domains	T1491.002 External Defacement	T1491 Defacement	T1104 Multi-Stage Channels
T1583.001 Domains	T1583 Acquire Infrastructure	T1585 Establish Accounts	T1593.001 Social Media
T1059.007 JavaScript	T1059 Command and Scripting Interpreter	T1027 Obfuscated Files or Information	T1585.001 Social Media Accounts

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	09474w.reyt-cre-ad34[.]buzz, 1wifsq.c-majac-ann4[.]buzz, 3wk8wa.kariz-good-ad10[.]buzz, 62ogyy[.]internetbusinesslondon[.]co[.]uk, 6fmb3r[.]great-cred195[.]buzz, allons-y[.]social, antiwar[.]com, arbeitspause[.]org, arizztar[.]com, bfmtv[.]com, bluetoffee-books[.]com, brennendefrage[.]com, buegym.ranking-kariz108[.]buzz, contre-attaque[.]net, d6egyr.borafazerfestaoficial[.]online, deintelligenz[.]com, derbayerischelowe[.]info, derglaube[.]com,

TYPE	VALUE
Domains	derrattenfanger[.]net, deutschlandkurier[.]de, faridmehdipour[.]com, faz[.]ltd, freeebooktemplates[.]com, freiewelt[.]net, ggspace[.]space, grunehummel[.]com, histoireetsociete[.]com, hungarianconservative[.]com, jungefreiheit[.]de, kaputteampel[.]com, ledialogue[.]fr, legrandsoir[.]info, leparisien[.]re, lildoxi[.]com, miastagebuch[.]com, mt-secure-bnk[.]com, nice-credits-list266[.]buzz, nw3m7o.samaritana.com[.]br, o21obd.reyt-credbest-mx29[.]buzz, osthessen-news[.]de, overton-magazin[.]de, pcrrjx.kredit-money-fun169[.]buzz, profesionalvirtual[.]com, realpeoplesreviews[.]com, referendud[.]com, restuapp[.]com, sbl63p.kredit-money-fun274[.]buzz, sdgqaef[.]site, sueddeutsche[.]ltd, telepolis[.]de, uncut-news[.]ch, v5yoaq.chilling[.]lol, voltairenet[.]org, wanderfalke[.]net, welt[.]pm, www.nachdenkseiten[.]de, yzrhhk.kredit-money-fun202[.]buzz

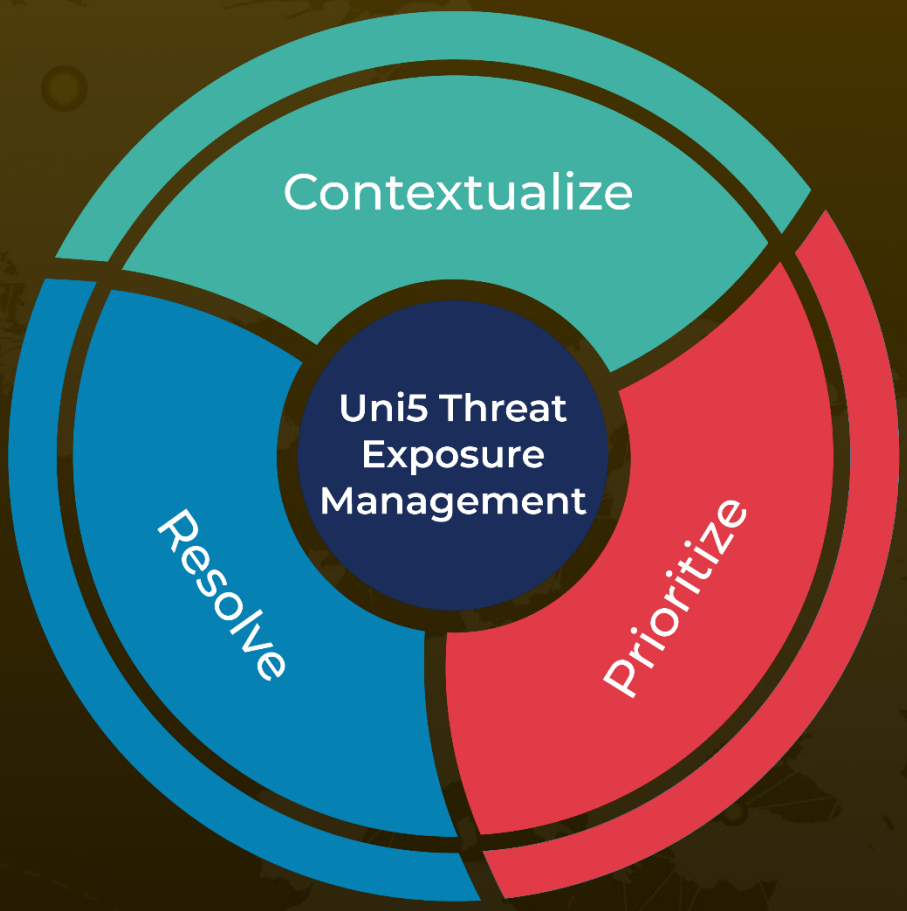
References

https://www.sentinelone.com/labs/doppelganger-russia-aligned-influence-operation-targets-germany/

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

February 27, 2024 • 7:30 AM

More at www.hivepro.com