Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

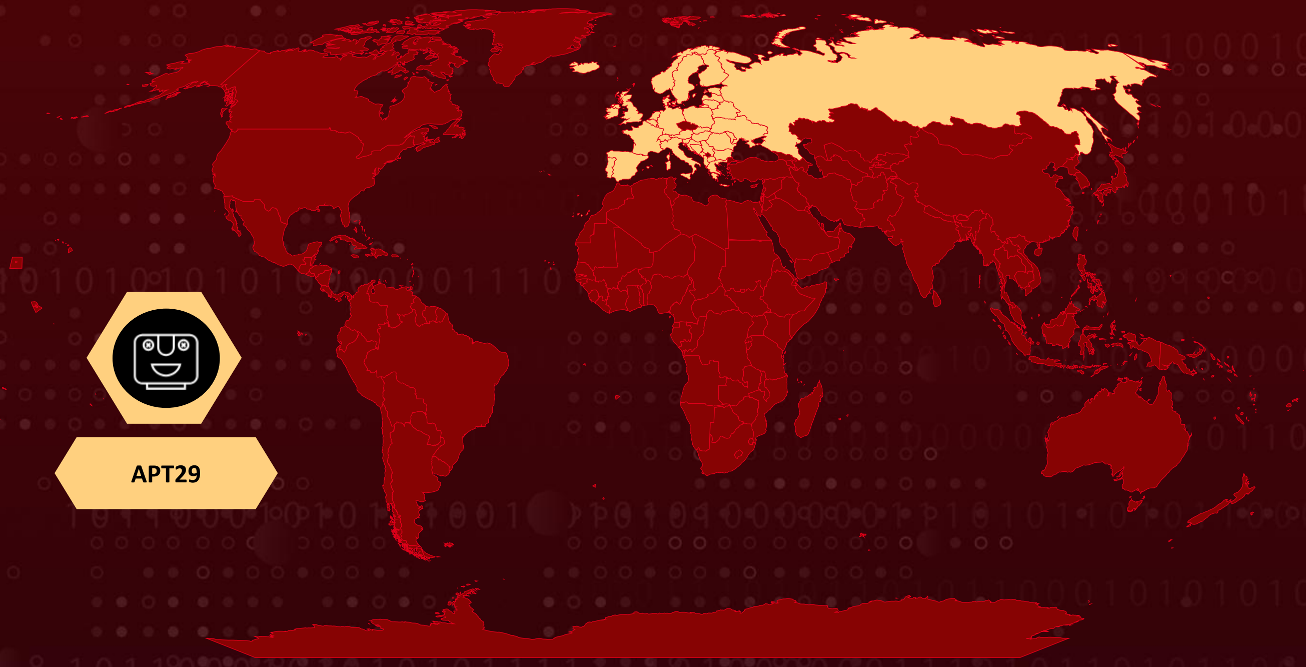
APT29 Deploys GRAPELOADER via Wine-Tasting Phishing Emails

Date of Publication	Admiralty Code	TA Number
April 16, 2025	A1	TA2025117

Summary

Attack Commenced: January 2025
Targeted Region: Europe
Targeted Platform: Windows
Threat Actor: APT29 (aka Cozy Bear, The Dukes, Group 100, Yttrium, Iron Hemlock, Minidionis, CloudLook, ATK 7, ITG11, Grizzly Steppe, UNC2452, Dark Halo, SolarStorm, StellarParticle, SilverFish, Nobelium, Iron Ritual, Cloaked Ursa, BlueBravo, ATK7, Blue Kitsune, G0016, Midnight Blizzard, SeaDuke, TA421, UAC-0029)
Malware: GRAPELOADER, WINELOADER
Targeted Industry: Embassies, Government, and Diplomatic entities
Attack: In early 2025, APT29 launched a targeted phishing campaign impersonating a European Ministry of Foreign Affairs, using wine-tasting event invitations to deliver malware. The attackers deployed a new loader called GRAPELOADER via DLL side-loading, establishing persistence and communicating with C2 servers. This loader then delivered the advanced WINELOADER backdoor, which uses strong encryption and anti-analysis techniques for stealthy data exfiltration. The campaign highlights APT29's evolving tactics targeting diplomatic and government entities with sophisticated malware and social engineering.

Attack Regions



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

Attack Details

#1

In early 2025, APT29 (also known as Cozy Bear or Midnight Blizzard), a Russian state-sponsored cyber espionage group, initiated a sophisticated phishing campaign targeting European diplomatic entities. The attackers impersonated a major European Ministry of Foreign Affairs, sending fake invitations to wine-tasting events to diplomats and embassy staff. These emails contained malicious links that, when clicked, led to the deployment of a new malware loader named GRAPELOADER.

#2

GRAPELOADER serves as the initial-stage loader in the attack chain, responsible for fingerprinting the victim's system, establishing persistence, and delivering subsequent payloads. It exhibits advanced stealth techniques and shares code similarities with the previously known WINELOADER, indicating a refinement in APT29's malware development.

#3

Following the initial compromise, the campaign transitions to a multi-stage backdoor framework. Researchers have identified a new variant of WINELOADER active in later phases, which retains its modular architecture: encrypted plugin modules are fetched on demand, decrypted in memory, and executed to perform reconnaissance, data exfiltration, or lateral movement. The use of both GRAPELOADER and WINELOADER suggests a multi-phase infection strategy aimed at maintaining long-term access to targeted systems.

#4

APT29's continued focus on high-profile targets, such as diplomatic missions and government agencies, underscores its role in cyber espionage activities aligned with Russian intelligence interests. The group's use of sophisticated social engineering tactics and custom malware highlights the evolving threat landscape and the need for heightened cybersecurity measures among potential targets.

#5

This campaign demonstrates APT29's ability to adapt and refine its techniques, employing advanced malware and deceptive lures to infiltrate sensitive networks. The discovery of GRAPELOADER and the updated WINELOADER variant provides valuable insights into the group's operational capabilities and emphasizes the importance of continuous monitoring and analysis to defend against such threats.

Recommendations

Strengthen Email Security: Implement advanced email filtering solutions capable of detecting and blocking phishing attempts, especially those involving spoofed domains and deceptive content. Enable DMARC, SPF, and DKIM to validate sender authenticity.

Deploy Advanced Endpoint Protection: Utilize Endpoint Detection and Response (EDR) tools to monitor for suspicious activities, such as DLL sideloading and unauthorized registry modifications, which are tactics employed by GRAPELOADER and WINELOADER. Ensure that all endpoints have up-to-date antivirus and anti-malware solutions to detect and prevent known threats.

Network & Host-Level Protections: Monitor for connections to known or newly registered malicious domains (like those mimicking foreign affairs ministries). Apply strict egress filtering to prevent malware from communicating freely with command-and-control servers. Segment sensitive networks and apply least-privilege access to limit lateral movement.

Potential MITRE ATT&CK TTPs

TA0007 Discovery	TA0005 Defense Evasion	TA0010 Exfiltration	TA0002 Execution
TA0003 Persistence	TA0001 Initial Access	TA0009 Collection	TA0011 Command and Control
T1566 Phishing	T1204 User Execution	T1204.001 Malicious Link	T1574.002 DLL Side-Loading

T1574 Hijack Execution Flow	**T1027** Obfuscated Files or Information	**T1140** Deobfuscate/Decode Files or Information	**T1005** Data from Local System
T1566.002 Spearphishing Link	**T1059.001** PowerShell	**T1059** Command and Scripting Interpreter	**T1218** System Binary Proxy Execution
T1016 System Network Configuration Discovery	**T1547.001** Registry Run Keys / Startup Folder	**T1547** Boot or Logon Autostart Execution	**T1041** Exfiltration Over C2 Channel
T1027.009 Embedded Payloads	**T1070.001** Clear Windows Event Logs	**T1070** Indicator Removal	**T1573.001** Symmetric Cryptography
T1573 Encrypted Channel	**T1071.001** Web Protocols	**T1071** Application Layer Protocol	**T1082** System Information Discovery
T1656 Impersonation			

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	a89b9bdf5f28f4380f383ee199401bdc, e025fa8354968f298af3f6ef2f22d7d3, e06fbace9c2297e47e6bf991f2681b2b, f474f6cd156e53a994ae3d25dcecb50c
SHA1	3a7b4a507db8ac2aa59c83a59dcf1242411d14f5, 56248469a7c079c4174f6c8351b48294bd7a57e0, 5a3bd2f12875098bd06b9f5a5a9405d9cf3af837, b4221c83a3fffe7bc358dfc613c3e58fcc522a23
SHA256	24c079b24851a5cc8f61565176bbf1157b9d5559c642e31139ab8d76bbb320f8, 420d20cddfaada4e96824a9184ac695800764961bad7654a6a6c3fe9b1b74b9a, 653db3b63bb0e8c2db675cd047b737cefebb1c955bd99e7a93899e2144d34358,

TYPE	VALUE
SHA256	78a810e47e288a6aff7ffbaf1f20144d2b317a1618bba840d42405cddc4cff41, 85484716a369b0bc2391b5f20cf11e4bd65497a34e7a275532b729573d6ef15e, adfe0ef4ef181c4b19437100153e9fe7aed119f5049e5489a36692757460b9f8, d931078b63d94726d4be5dc1a00324275b53b935b77d3eed1712461f0c180164
URLs	hxxps[://]bakenhof[.]com/invb[.]php, hxxps[://]silry[.]com/inva[.]php
Domains	bakenhof[.]com, bravecup[.]com, ophibre[.]com, silry[.]com

References

https://research.checkpoint.com/2025/apt29-phishing-campaign/

https://www.hivepro.com/threat-advisory/apt29-a-deep-dive-into-russias-cyber-espionage/

https://www.hivepro.com/threat-advisory/apt29-targets-german-political-parties-with-new-wineloader/

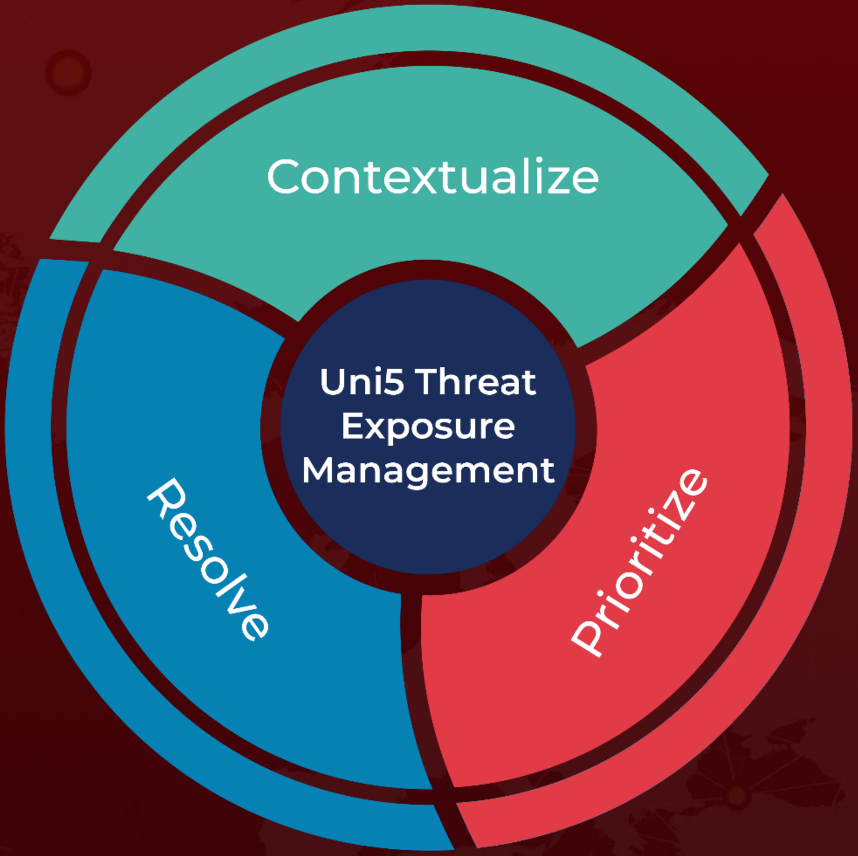
https://attack.mitre.org/groups/G0016/

https://cloud.google.com/blog/topics/threat-intelligence/apt29-wineloader-german-political-parties

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

April 16, 2025 • 11:00 PM

More at www.hivepro.com