Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

⚔ ATTACK REPORT

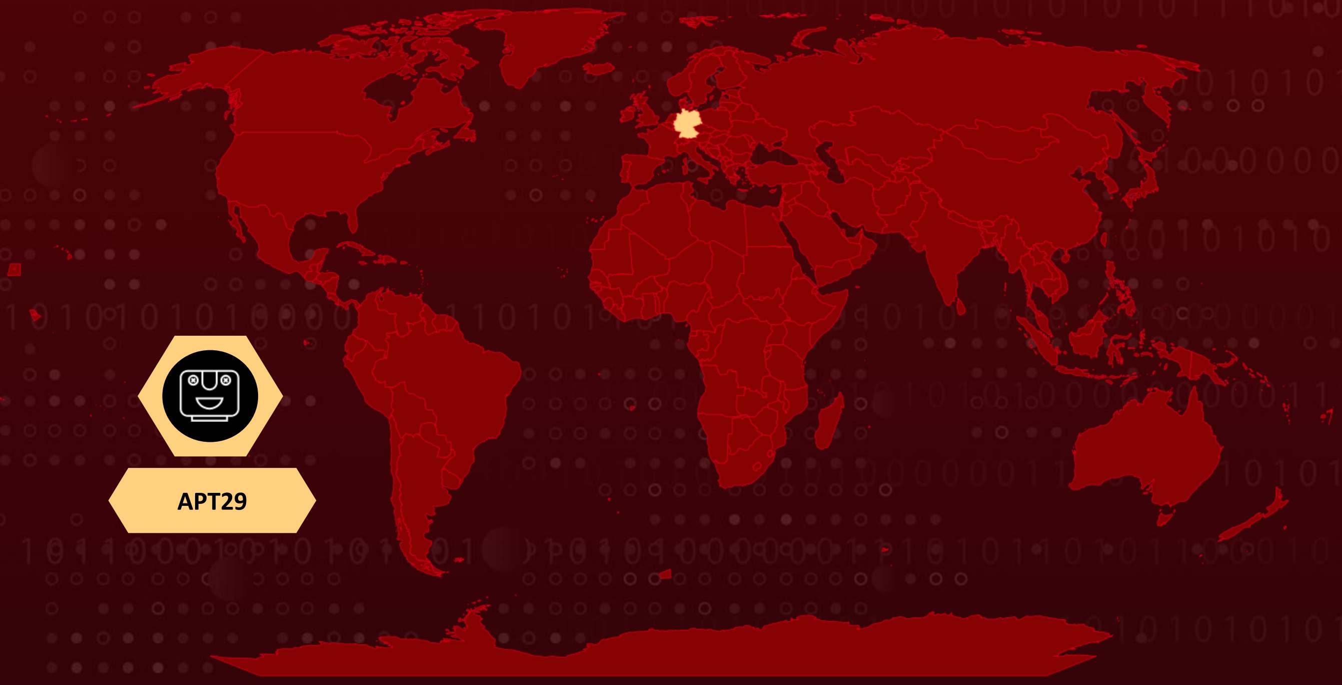
APT29 Targets German Political Parties with New WINELOADER

Date of Publication	Admiralty Code	TA Number
March 26, 2024	A1	TA2024116

Summary

Attack Began: February 26, 2024
Targeted Countries: Germany
Threat Actor: APT29
Malware: WINELOADER, ROOTSAW
Targeted Industries: Diplomatic, Political, Government, and Civil Society
Affected Platform: Windows
Attack: APT29, linked to Russia's SVR, targeted German political parties in late February 2024 using a new backdoor variant named WINELOADER, signaling a shift in operational focus beyond diplomatic missions. This marks a broader threat to European and Western political entities, driven by the SVR's interest in political intelligence collection.

Attack Regions


APT29
Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

Attack Details

#1

In late February 2024, APT29, a Russian-backed threat group associated with Russia's Foreign Intelligence Service (SVR), launched a phishing campaign targeting German political parties. This operation marked a shift for APT29, which typically targeted governmental and diplomatic entities. They used a new backdoor variant called WINELOADER, observed for the first time in an operation targeting diplomatic entities across several countries earlier this year.

#2

The phishing emails pretended to be invitations to a dinner reception, bearing the logo of the Christian Democratic Union (CDU), a major German political party. Victims were directed to a malicious ZIP file containing a first-stage payload called ROOTSAW, hosted on an actor-controlled compromised website. ROOTSAW then delivered a CDU-themed lure document and the WINELOADER payload.

#3

WINELOADER, observed for the first time in January 2024, shares characteristics with other APT29 malware families like BURNTBATTER and MUSKYBEAT, suggesting a common developer. It communicates with its command-and-control server via HTTP GET requests, allowing the attackers to execute commands and update settings on compromised systems.

#4

This activity indicates a broader threat to European and Western political parties, as APT29's interest expands beyond diplomatic missions. Their operations are highly adaptive and likely to target political organizations beyond Germany. Additionally, a number of APT29 subclusters have shift in their tactics with speculation involving subvert of cloud-based authentication mechanisms or password spraying to gain initial access. This highlights the ongoing need for vigilance and cybersecurity measures among political entities.

Recommendations

Endpoint Protection: Deploy and regularly update endpoint protection software to detect and prevent the execution of malicious payloads like WINELOADER. Utilize advanced threat detection mechanisms capable of identifying and blocking sophisticated malware.

Access Control and Authentication: Deploy strong access controls and authentication mechanisms to prevent unauthorized access to sensitive systems and data. Enforce the principle of least privilege to limit user access rights and privileges to only those necessary for their role.

Email Security Measures: Deploy email security solutions to detect and block phishing emails, malware attachments, and suspicious URLs. Implement email authentication protocols such as SPF, DKIM, and DMARC to prevent email spoofing and impersonation attacks.

Network Monitoring and Intrusion Detection: Deploy network monitoring and intrusion detection systems to detect anomalous behavior and potential indicators of compromise. Monitor network traffic for signs of reconnaissance, lateral movement, and data exfiltration associated with APT campaigns like APT29.

Potential MITRE ATT&CK TTPs

TA0007 Discovery	TA0011 Command and Control	TA0001 Initial Access	TA0002 Execution
TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0006 Credential Access
T1543.003 Windows Service	T1543 Create or Modify System Process	T1012 Query Registry	T1082 System Information Discovery
T1134 Access Token Manipulation	T1057 Process Discovery	T1007 System Service Discovery	T1027 Obfuscated Files or Information
T1070.004 File Deletion	T1070 Indicator Removal	T1055.003 Thread Execution Hijacking	T1055 Process Injection

T1083 File and Directory Discovery	T1071.001 Web Protocols	T1071 Application Layer Protocol	T1574.002 DLL Side-Loading
T1574 Hijack Execution Flow	T1566 Phishing	T1110 Brute Force	T1110.003 Password Spraying
T1566.002 Spearphishing Link	T1204.002 Malicious File	T1204 User Execution	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	A0f183ea54cb25dd8bdba586935a258f0ecd3cba0d94657985bb1ea02af8d42c
SHA1	5b6b25012fa541a227e1c20d9f3004ce4e7d4aee
MD5	44ce4b785d1795b71cee9f77db6ffe1b, 5928907c41368d6e87dc3e4e4be30e42, 7a465344a58a6c67d5a733a815ef4cb7, 8bd528d2b828c9289d9063eba2dc6aa0, e017bfc36e387e8c3e7a338782805dde, efafcd00b9157b4146506bd381326f39, fb6323c19d3399ba94ecd391f7e35a9c
URLs	http://waterforvoiceless[.]org/invite[.]xn--php-9o0a, http://waterforvoiceless[.]org/util[.]xn--php-9o0a[.], https://siestakeying[.]com/auth[.]php, https://waterforvoiceless[.]org/invite[.]php, https://waterforvoiceless[.]org/invite[.]xn--php-9o0a[.], https://waterforvoiceless[.]org/util[.]php
Domains	0x3bd487[.]open, siestakeying[.]com, waterforvoiceless[.]org

References

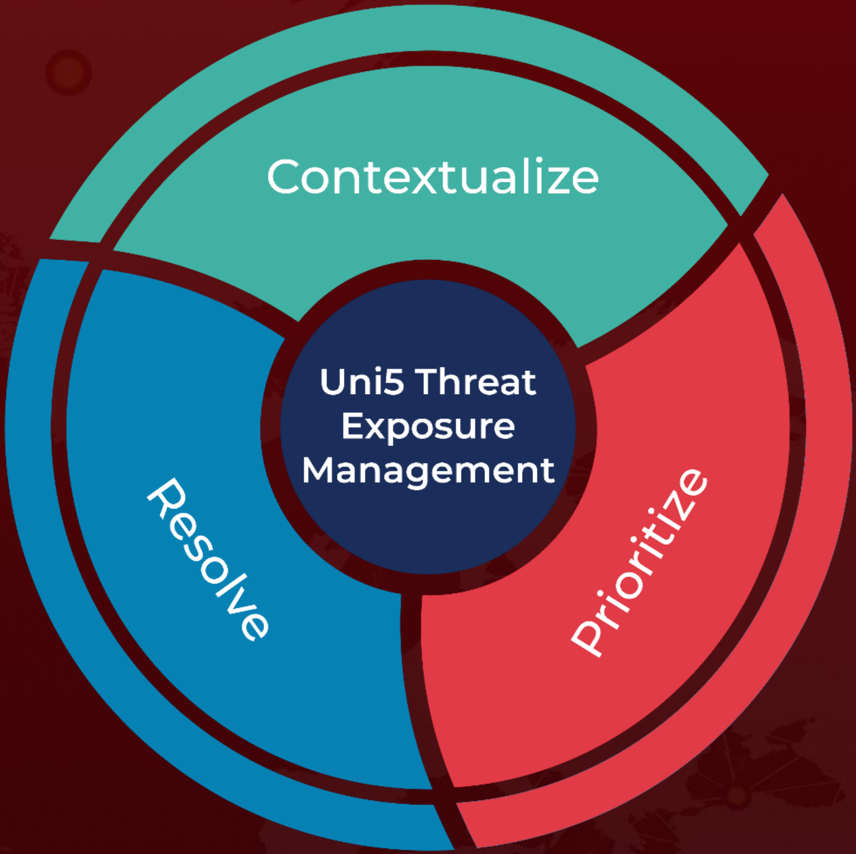
https://www.mandiant.com/resources/blog/apt29-wineloader-german-political-parties

https://www.hivepro.com/threat-advisory/spikedwine-ploy-to-infiltrate-eu-diplomatic-circles/

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

March 26, 2024 • 5:30 AM

More at www.hivepro.com