Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ACTOR REPORT

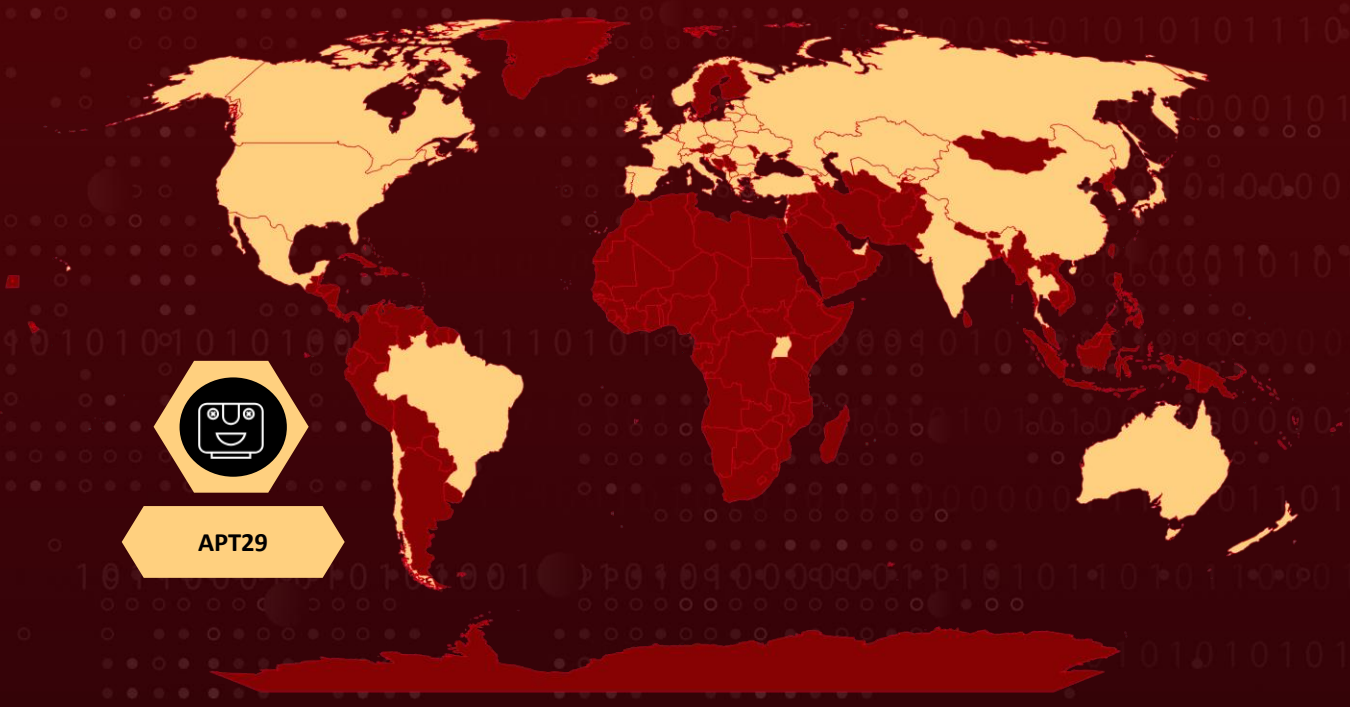
APT29: A Deep Dive into Russia's Cyber Espionage

Date of Publication	Admiralty code	TA Number
July 4, 2024	A1	TA2024255

Summary

First Appearance: 2008
Actor Name: 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)
Targeted Regions: Australia, Azerbaijan, Belarus, Belgium, Brazil, Canada, Chechnya, Chile, China, Cyprus, Czech, Denmark, France, Georgia, Germany, India, Ireland, Israel, Italy, Japan, Kazakhstan, Kyrgyzstan, Lebanon, Luxembourg, Mexico, Netherlands, New Zealand, Portugal, Russia, Singapore, Spain, South Korea, Switzerland, Thailand, Turkey, Uganda, UAE, UK, Ukraine, USA, Uzbekistan, NATO
Malware: WINELOADER, RootSaw, VaporRage
Targeted Industry: Aerospace, Defense, Education, Embassies, Energy, Financial, Government, Healthcare, Law enforcement, Media, NGOs, Pharmaceutical, Telecommunications, Transportation, Think Tanks and Technology

Actor Map



Attack Details

#1

APT29, also known as "Cozy Bear," is a cyber espionage group associated with the Russian Foreign Intelligence Service (SVR). Active since 2008, APT29 conducts advanced persistent threat (APT) operations involving prolonged, targeted cyber attacks against high-value targets, impacting diplomatic relations and national security.

#2

APT29 employs sophisticated tactics, techniques, and procedures (TTPs), often using spear phishing campaigns to deliver various malware types, recently targeting inactive cloud service accounts for initial access. These emails typically contain malicious attachments or links that, when opened, enable long-term access and data exfiltration. They use custom malware like "CosmicDuke," "MiniDuke," "WellMess," and "WellMail," which work on Windows and Linux and use cryptography and anti-analysis techniques.

#3

The group excels in evading detection by using encryption, polymorphic code, and legitimate tools and credentials within compromised networks. Once inside, APT29 moves laterally and escalates privileges using stolen credentials and software vulnerabilities.APT29 has been linked to several high-profile campaigns. In the 2016 U.S. presidential election, alongside APT28 (Fancy Bear), they hacked the Democratic National Committee (DNC).

#4

In 2020, APT29 was involved in the SolarWinds supply chain attack, compromising SolarWinds' Orion software and infiltrating numerous high-profile organizations, including U.S. government agencies. Additionally, in mid-2020, APT29 targeted COVID-19 vaccine development efforts in Canada, the UK, and the U.S. using WellMess and WellMail tools.

#5

In late February 2024, APT29 shifted tactics to target German political parties with a new backdoor variant named WINELOADER, marking a shift from their usual diplomatic focus to political intelligence collection. APT29 recently breached TeamViewer's corporate network, likely using stolen employee login credentials. This led to the exfiltration of employee records, including names, contact details, and encrypted passwords. However, customer data was protected and remains unaffected.

#6

APT29's evolving tactics and high-profile targets make them a significant concern. The TeamViewer incident in June 2024 exemplifies their determination and calls for adoption of proactive cybersecurity measures.

Actor Group

NAME	ORIGIN	TARGET REGIONS	TARGET INDUSTRIES
APT29	Russia **MOTIVE** Espionage and Information theft	Australia, Azerbaijan, Belarus, Belgium, Brazil, Bulgaria, Canada, Chechnya, Chile, China, Cyprus, Czech, Denmark, France, Georgia, Germany, Hungary, India, Ireland, Israel, Italy, Japan, Kazakhstan, Kyrgyzstan, Latvia, Lebanon, Lithuania, Luxembourg, Mexico, Montenegro, Netherlands, New Zealand, Poland, Portugal, Romania, Russia, Singapore, Slovakia, Slovenia, Spain, South Korea, Switzerland, Thailand, Turkey, Uganda, UAE, UK, Ukraine, USA, Uzbekistan, NATO	Aerospace, Defense, Education, Embassies, Energy, Financial, Government, Healthcare, Law enforcement, Media, NGOs, Pharmaceutical, Telecommunications, Transportation, Think Tanks and Imagery

Recommendations

Implement Email Security Solutions: Deploy email filtering and security solutions to detect and block phishing emails containing malicious attachments or links. Educate employees on recognizing phishing attempts.

Threat Exposure Management: Implement a robust threat exposure management framework to continuously assess, prioritize, and mitigate cybersecurity risks across the organization's digital footprint.

Zero-Trust Architecture: Adopt a Zero-Trust approach by verifying every request as though it originates from an open network, regardless of whether it originates from inside or outside the network perimeter. Implement strict access controls based on identity, device health, and other contextual factors.

Security-by-Design Principles: Incorporate security considerations into the design and development phases of systems and applications. Follow secure coding practices, conduct architecture reviews, and integrate automated security testing tools into the CI/CD pipeline.

Advanced Threat Detection and Response: Deploying advanced threat detection and response solutions is essential for identifying and mitigating sophisticated attacks. This includes using Endpoint Detection and Response (EDR) tools, Intrusion Detection Systems (IDS), and Intrusion Prevention Systems (IPS). These tools can detect unusual activity and provide alerts on potential intrusions, allowing for quicker response times.

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
T1566.002 Spearphishing Link	**T1204.002** Malicious File	**T1204** User Execution	**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
T1078.004 Cloud Accounts	**T1528** Steal Application Access Token	**T1078** Valid Accounts	**T1621** Multi-Factor Authentication Request Generation
T1543.003 Windows Service	**T1543** Create or Modify System Process	**T1012** Query Registry	**T1098.005** Device Registration
T1098 Account Manipulation	**T1651** Cloud Administration Command	**T1059.009** Cloud API	**T1059** Command and Scripting Interpreter

Indicator of Compromise (IOCs)

TYPE	VALUE
SHA256	A0f183ea54cb25dd8bdba586935a258f0ecd3cba0d94657985bb1ea02af8d42c, d0a8fa332950b72968bdd1c8a1a0824dd479220d044e8c89a7dea4434b741750, 1c7593078f69f642b3442dc558cddff4347334ed7c96cd096367afd08dca67bc, 3739b2eae11c8367b576869b68d502b97676fb68d18cc0045f661fbe354afcb9, 72b92683052e0c813890caf7b4f8bfd331a8b2afc324dd545d46138f677178c4, 7600d4bb4e159b38408cb4f3a4fa19a5526eec0051c8c508ef1045f75b0f6083, ad43bbb21e2524a71bad5312a7b74af223090a8375f586d65ff239410bbd81a7, b014cdff3ac877bdd329ca0c02bdd604817e7af36ad82f912132c50355af0920, c1223aa67a72e6c4a9a61bf3733b68bfbe08add41b73ad133a7c640ba265a19e, e477f52a5f67830d81cf417434991fe088bfec21984514a5ee22c1bcffe1f2bc, f61cee951b7024fca048175ca0606bfd550437f5ba2824c50d10bef8fb54ca45, c7b01242d2e15c3da0f45b8adec4e6913e534849cde16a2a6c480045e03fbee4, 7b666b978dbbe7c032cef19a90993e8e4922b743ee839632bfa6d99314ea6c53, ebe231c90fad02590fc56d5840acc63b90312b0e2fee7da3c7606027ed92600e, 773f0102720af2957859d6930cd09693824d87db705b3303cef9ee794375ce13,
SHA1	5b6b25012fa541a227e1c20d9f3004ce4e7d4aee
MD5	44ce4b785d1795b71cee9f77db6ffe1b, 5928907c41368d6e87dc3e4e4be30e42, 7a465344a58a6c67d5a733a815ef4cb7, 8bd528d2b828c9289d9063eba2dc6aa0, e017bfc36e387e8c3e7a338782805dde, efafcd00b9157b4146506bd381326f39, fb6323c19d3399ba94ecd391f7e35a9c

TYPE	VALUE
URLs	hxxp://waterforvoiceless[.]org/invite[.]xn--php-9o0a, hxxp://waterforvoiceless[.]org/util[.]xn--php-9o0a[.], hxxps://siestakeying[.]com/auth[.]php, hxxps://waterforvoiceless[.]org/invite[.]php, hxxps://waterforvoiceless[.]org/invite[.]xn--php-9o0a[.], hxxps://waterforvoiceless[.]org/util[.]php
Domains	0x3bd487[.]open, siestakeying[.]com, waterforvoiceless[.]org

References

https://www.nccgroup.com/uk/newsroom/threat-intelligence-teamviewer-compromised-by-apt29/

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

https://www.techtarget.com/searchsecurity/news/366571396/CISA-APT29-targeting-cloud-accounts-for-initial-access

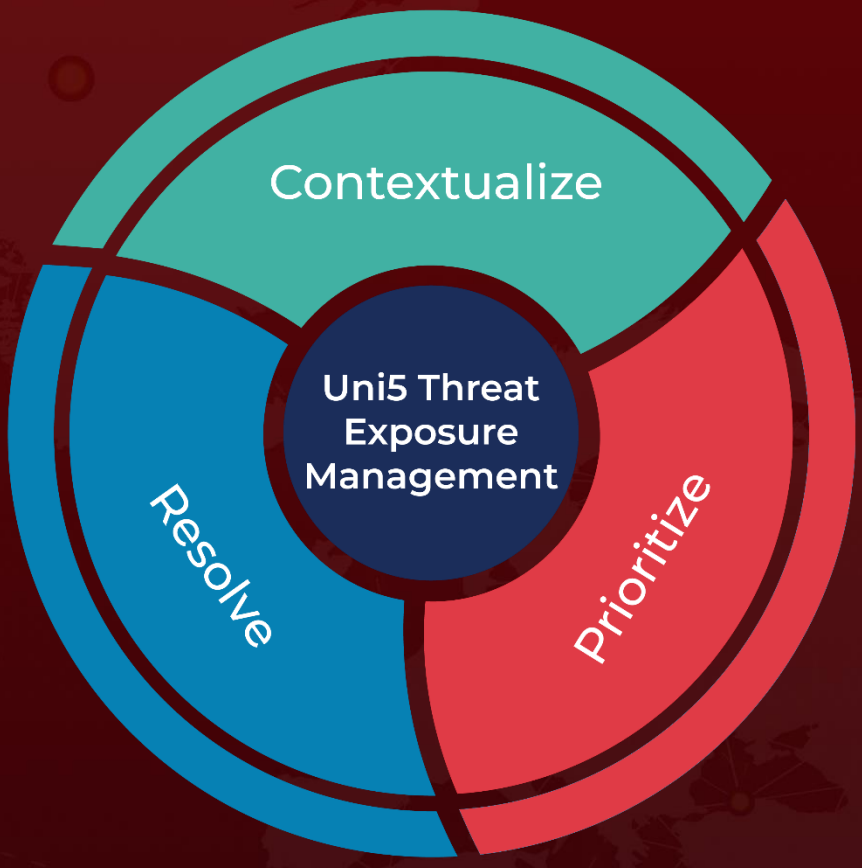
https://attack.mitre.org/groups/G0016/

https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-057a

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

July 4, 2024 • 4:30 AM

More at www.hivepro.com