Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

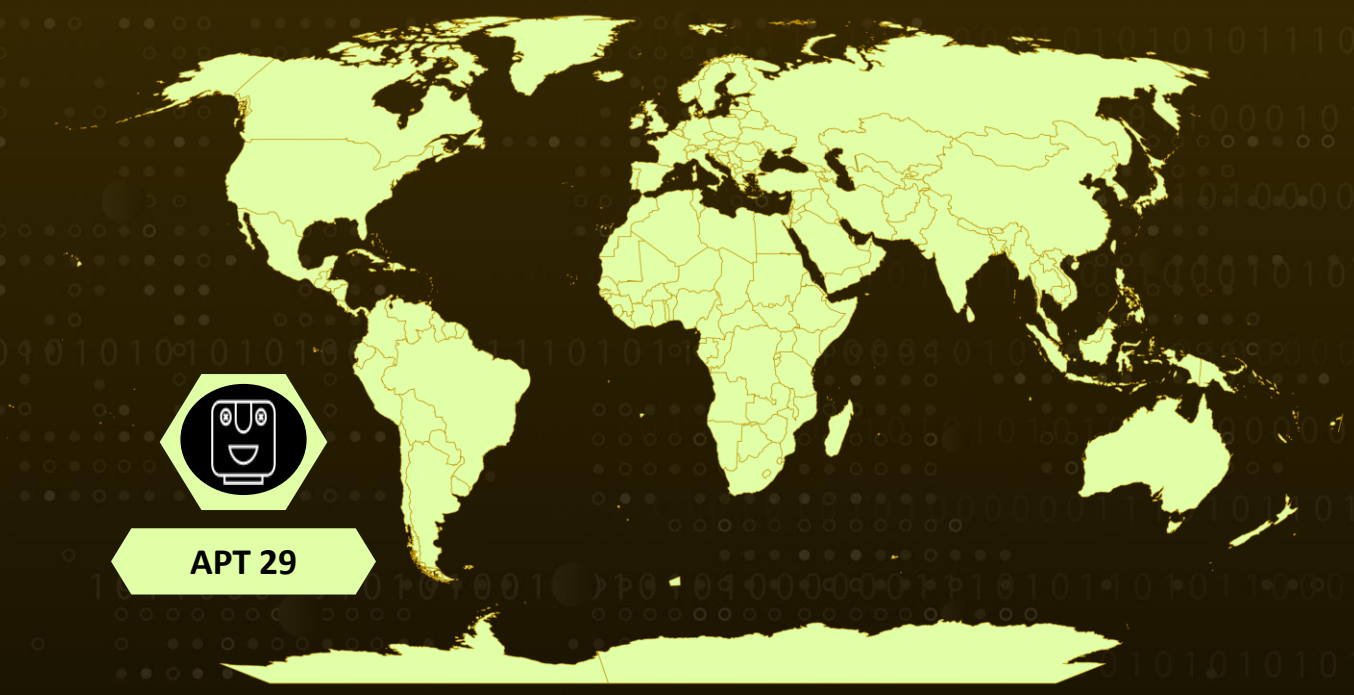
New APT 29 Campaign Targets Organizations through Microsoft Teams

Date of Publication	Admiralty Code	TA Number
August 3, 2023	A1	TA2023320

Summary

First appeared: May 2023
Attack Region: Worldwide
Actor Name: APT 29 (aka Midnight Blizzard, 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)
Affected Platform: Windows
Targeted Industries: Government, Non-Government Organizations (NGOs), IT services, Technology, Discrete manufacturing, and Media
Attack: APT 29, a Russia-based threat actor, employs targeted social engineering via Microsoft Teams to steal credentials, leveraging compromised domains and convincing users to enter authentication codes, furthering their espionage objectives.

Attack Regions



Attack Details

#1 A targeted credential theft phishing attack conducted via Microsoft Teams chats by a threat group referred to as APT 29 (aka Midnight Blizzard). This represents part of their ongoing efforts using both new and familiar techniques.

#2 The attacker's current method involves creating security-themed domains hosted on compromised tenants to trick users into providing authentication codes. The attack chain includes Teams messages masquerading as technical support, convincing users to enter authentication codes into the Microsoft Authenticator app, and granting the attacker access to compromised accounts.

#3 This activity underscores the persistent threat of APT 29's espionage-focused attacks using evolving techniques. Around 40 global organizations have been affected by this campaign, targeting government, NGO, IT, tech, manufacturing, and media sectors.

#4 APT 29 is associated with the Russian Foreign Intelligence Service (SVR). They focus on espionage and have targeted governments, NGOs, and IT service providers, primarily in the US and Europe. Their tactics involve various initial access methods, from stolen credentials to supply chain attacks, and they are known for their consistency and persistence in targeting.

Recommendations

- Deploy advanced authentication methods like hardware tokens or biometrics to enhance security against phishing attempts and unauthorized access.
- Enforce stronger authentication, such as multi-factor authentication (MFA), through Conditional Access policies for critical applications, adding an extra layer of protection.
- Regularly train employees on security best practices, emphasizing the risks of phishing attacks and malicious downloads, to minimize the likelihood of falling victim to attacks by the APT 29 Group or other threat actors.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0006 Credential Access	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0040 Impact	TA0009 Collection	TA0042 Resource Development
T1036 Masquerading	T1621 Multi-Factor Authentication Request Generation	T1566 Phishing	T1110.003 Password Spraying
T1110 Brute Force	T1484.002 Domain Trust Modification	T1484 Domain Policy Modification	T1583.001 Domains
T1583 Acquire Infrastructure	T1566.003 Spearphishing via Service	T1586 Compromise Accounts	T1530 Data from Cloud Storage

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	msftprotection.onmicrosoft[.]com identityVerification.onmicrosoft[.]com accountsVerification.onmicrosoft[.]com azuresecuritycenter.onmicrosoft[.]com teamsprotection.onmicrosoft[.]com

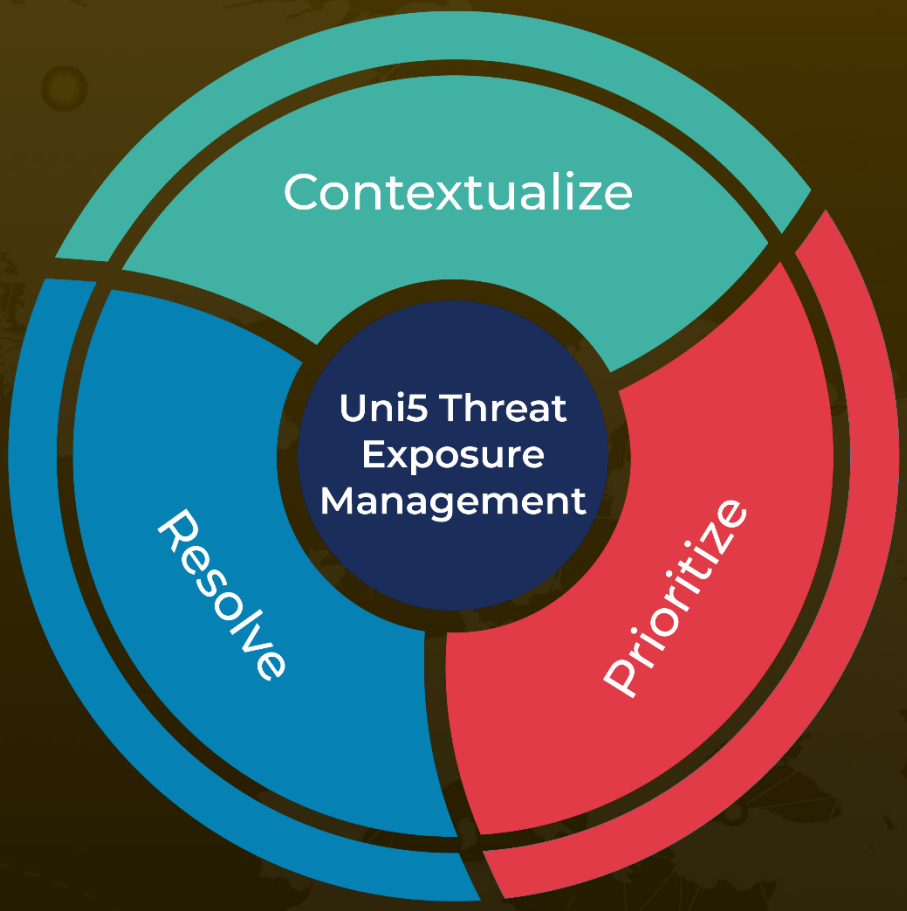
References

https://www.microsoft.com/en-us/security/blog/2023/08/02/midnight-blizzard-conducts-targeted-social-engineering-over-microsoft-teams/

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

August 3, 2023 • 7:10 AM

More at www.hivepro.com