Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

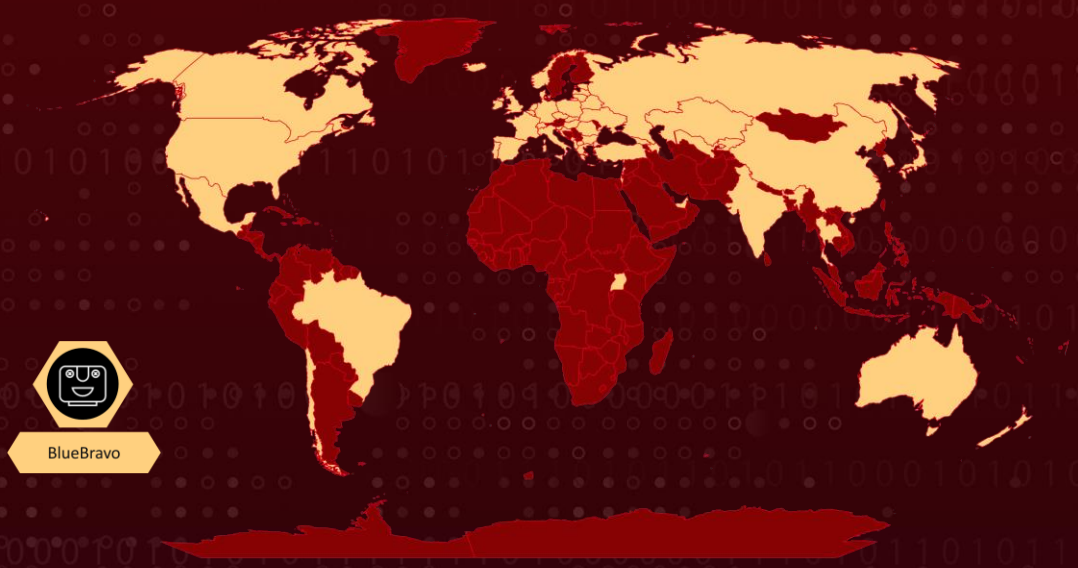
Uncovering the Threat of BlueBravo with GraphicalNeutrino and BEATDROP

Date of Publication	Admiralty Code	TA Number
February 1, 2023	A1	TA2023055

Summary

Attack Begin: October 2022
Threat Actor: BlueBravo (APT 29, 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)
Attack Countries: 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
Attack Sector: Aerospace, Defense, Education, Energy, Financial, Government, Healthcare, Law enforcement, Media, NGOs, Pharmaceutical, Telecommunications, Transportation, Think Tanks and Imagery
Attack: GraphicalNeutrino and BEATDROP are malicious software used by the Russian-linked threat group BlueBravo in targeted cyber attacks, using legitimate Western services for command-and-control communications to evade detection.

Attack Regions



Attack Details

#1

BlueBravo is a newly identified threat group believed to be connected to APT29 and NOBELIUM, which are Russian advanced persistent threat (APT) activities linked to Russia's Foreign Intelligence Service (SVR). In October 2022, BlueBravo was found to use GraphicalNeutrino malware, delivered via a malicious ZIP file. The targets of the attack appear to be embassy personnel or an ambassador, based on the lure of a hacked website with the text "Ambassador's schedule November 2022".

#2

The malware BEATDROP uses trello[.]com for command-and-control (C2) communication, while GraphicalNeutrino uses Notion, a US business automation service, for C2. BlueBravo's use of legitimate Western services to blend its malware traffic helps evade detection. Countries with links to the ongoing conflict in Ukraine are at increased risk of being targeted, given BlueBravo's tactics, techniques, and procedures align with APT29 and NOBELIUM's focus on foreign espionage, active measures, and electronic surveillance.

Recommendations

Security Leaders

Phishing simulations and routine education and awareness training and communications rarely account for MFA fatigue and web browser hygiene. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize and block all indicators attributed to the threat actors and attacks through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.
- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' & 'Indicators of Compromise (IoC)' on the following pages.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0007 Discovery	TA0011 Command and Control	T1584 Compromise Infrastructure	T1204 User Execution
T1204.002 Malicious File	T1547 Boot or Logon Autostart Execution	T1547.001 Registry Run Keys / Startup Folder	T1027 Obfuscated Files or Information
T1027.006 HTML Smuggling	T1027.007 Dynamic API Resolution	T1036 Masquerading	T1036.002 Right-to-Left Override
T1036.005 Match Legitimate Name or Location	T1140 Deobfuscate/Decode Files or Information	T1574 Hijack Execution Flow	T1574.001 DLL Search Order Hijacking
T1574.002 DLL Side-Loading	T1562 Impair Defenses	T1562.001 Disable or Modify Tools	T1033 System Owner/User Discovery
T1082 System Information Discovery	T1071 Application Layer Protocol	T1071.001 Web Protocols	T1102 Web Service
T1102.002 Bidirectional Communication	T1105 Ingress Tool Transfer		

Indicator of Compromise (IOCs)

TYPE	VALUE
Domains	totalmassasje[.]no
Files	140runtime.dll 7za.dll november_schedulexe.pdf photos_and_price.exe schedule.zip vcruntime140.dll

TYPE	VALUE
SHA256	1cffaf3be725d1514c87c328ca578d5df1a86ea3b488e9586f9db89d992da5c4 381a3c6c7e119f58dfde6f03a9890353a20badfa1bfa7c38ede62c6b0692103c 844e902977b478eace8568f49dd9e5c91db8e534f3c5410ee663d0be02bdf7e3 a0c3e6cd167b93f4646a7a3f2d46ed8bd4888d861b533662a66ca9711d49db1f cf160175c661efd4b1e1eecadf5f00f7203ef4c7445e36e3373d50b26086c552

References

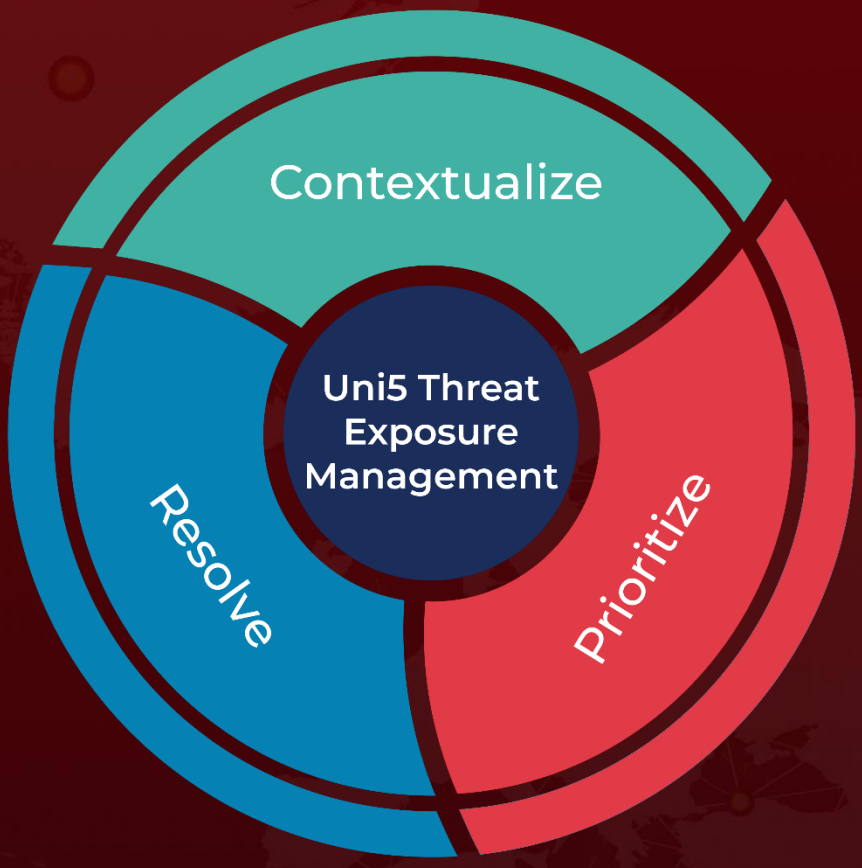
https://otx.alienvault.com/pulse/63d95dd289e5b68a19e9c791

https://go.recordedfuture.com/hubfs/reports/cta-2023-0127.pdf

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 1, 2023 • 2:15 AM

More at www.hivepro.com