Hive Pro

Threat Level

Red

HiveForce Labs

# THREAT ADVISORY

## ATTACK REPORT

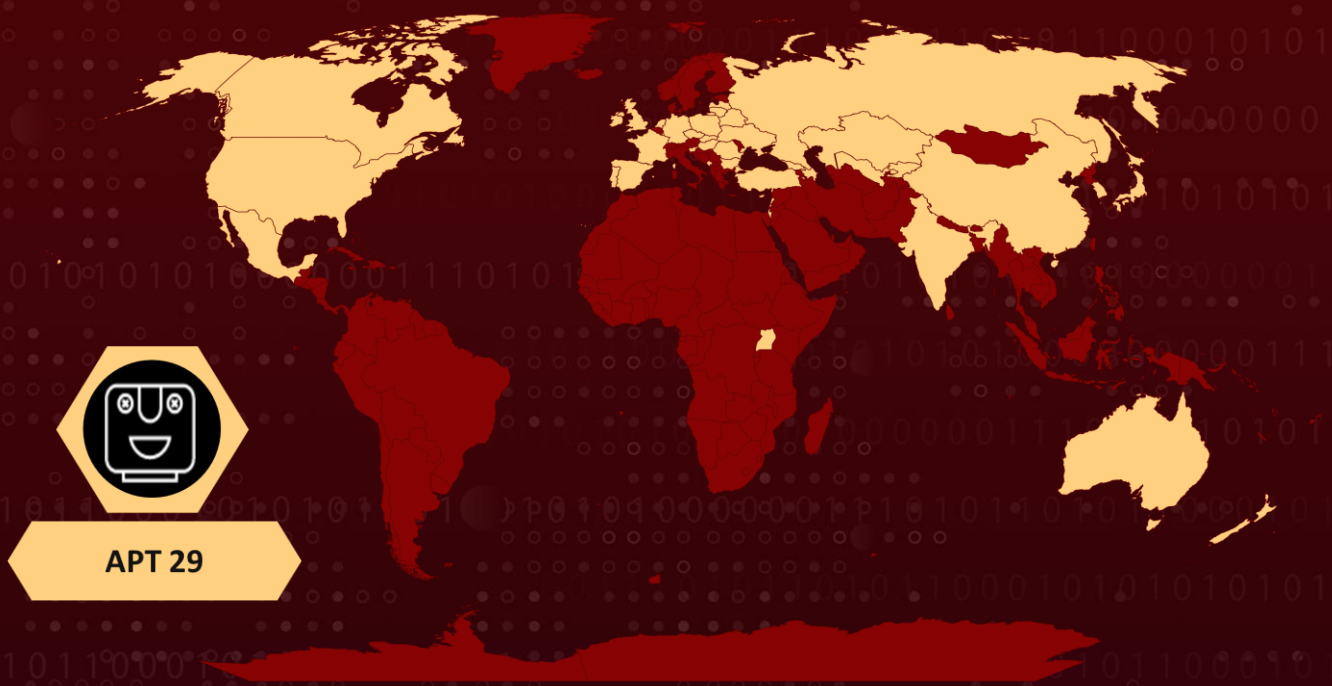
# APT 29 Launches Malevolent Campaign Targeting Governments

| Date of Publication | Admiralty Code | TA Number |
| --- | --- | --- |
| March 16, 2023 | A1 | TA2023140 |

# Summary

**Attack began:** January 2023
**Malware:** ROOTSAW (EnvyScout)
**Actor:** 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, BlueBravo)
**Attack Region:** Australia, Azerbaijan, Belarus, Belgium Brazil, Bulgaria, Canada, Chechnya, China, Cyprus, Czech, France, Georgia, Germany, Hungary, India, Ireland, Israel, Japan, Kazakhstan, Kyrgyzstan, Latvia, Lebanon, Lithuania, Luxembourg, Mexico, Montenegro, Netherlands, New Zealand, Poland, Portugal, Romania, Russia, Slovakia, Slovenia, Spain, South Korea, Turkey, Uganda, UK, Ukraine, USA, Uzbekistan.
**Targeted Industries:** Defense, Energy, Government, Law enforcement, Media, NGOs, Pharmaceutical, Telecommunications, Transportation, Think Tanks, and Imagery.
**Attack:** APT 29 has launched a novel campaign targeting Western countries. This latest operation involves the use of a malevolent dropper called ROOTSAW.

## Attack Regions



# Attack Details

**#1**

APT 29 is a Russian advanced persistent threat (APT) group that primarily engages in cyber espionage. In a recently detected operation targeting EU governments, the group was observed employing phishing emails that carried a malevolent document, leveraging the recent visit of the Polish Foreign Minister to the US as a pretext. Another tactic utilized by the group involves exploiting various legitimate systems, such as LegisWrite and eTrustEx.

**#2**

The malevolent document contains a hyperlink that leads to the download of an HTML file. Subsequently, the HTML file exposes APT 29's malicious dropper, which is tracked as ROOTSAW (also known as EnvyScout). ROOTSAW employs a technique called HTML smuggling to transmit an IMG or ISO file to the targeted system. The malware's objective is to gather and extract information about the compromised system, which it then dispatches to the Notion API for the command-and-control (C2) server.

# 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<br>Resource Development | TA0001<br>Initial Access | TA0002<br>Execution | TA0003<br>Persistence |
| TA0005<br>Defense Evasion | TA0011<br>Command and Control | T1584<br>Compromise Infrastructure | T1584.006<br>Web Services |
| T1566<br>Phishing | T1566.002<br>Spearphishing Link | T1204<br>User Execution | T1204.002<br>Malicious File |
| T1547<br>Boot or Logon Autostart Execution | T1547.001<br>Registry Run Keys / Startup Folder | T1027<br>Obfuscated Files or Information | T1027.006<br>HTML Smuggling |
| T1102<br>Web Service | T1102.002<br>Bidirectional Communication | | |

# Indicators of Compromise (IOCs)

| TYPE | VALUE |
|---|---|
| URL | hxxps[:]//literaturaelsalvador[.]com/Instructions[.]html<br>hxxps[:]//literaturaelsalvador[.]com/Schedule[.]html |
| IPV4 | 108[.]167.180[.]186 |
| MD5 | 67a6774fbc01eb838db364d4aa946a98<br>E693777A3A85583A1BBBD569415BE09C<br>89f716d32461880cd0359ffbb902f06e<br>e0cb8157e6791390463714b38158195a<br>cf36bf564fbb7d5ec4cec9b0f185f6c9<br>8d5c0f69c1caa29f8990fbc440ab3388<br>82ecb8474efe5fedcb8f57b8aafa93d2<br>38b05aa4b5ba651ba95f7173c5145270 |

| TYPE | VALUE |
| --- | --- |
| SHA256 | 21a0b617431850a9ea2698515c277cbd95de4e59c493d0d8f194f3808eb16354<br>505f1e5aed542e8bfdb0052bbe8d3a2a9b08fc66ae49efbc9d9188a44c3870ed<br>c1ebaee855b5d9b67657f45d6d764f3c1e46c1fa6214329a3b51d14eba336256<br>dbb39c2f143265ad86946d1c016226b0e01614af35a2c666afa44ac43b76b276<br>e957326b2167fa7ccd508cbf531779a28bfce75eb2635ab81826a522979aeb98<br>3a489ef91058620951cb185ec548b67f2b8d047e6fdb7638645ec092fc89a835<br>4d92a4cecb62d237647a20d2cdfd944d5a29c1a14b274d729e9c8ccca1f0b68b<br>dffaefaabbcf6da029f927e67e38c0d1e6271bf998040cfd6d8c50a4eff639df |

## References

https://blogs.blackberry.com/en/2023/03/nobelium-targets-eu-governments-assisting-ukraine

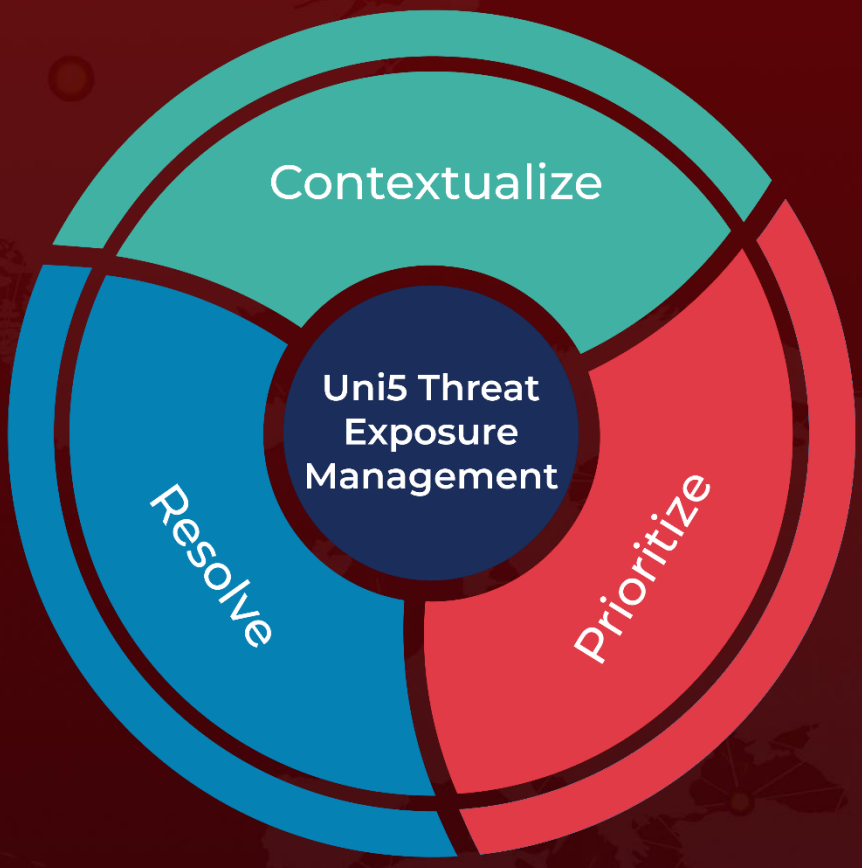
https://attack.mitre.org/groups/G0016/

https://attack.mitre.org/software/S0634/

# 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 16, 2023 • 2:32 AM**



More at www.hivepro.com