Hive Pro

Threat Level

Red

THREAT ADVISORY

ACTOR REPORT

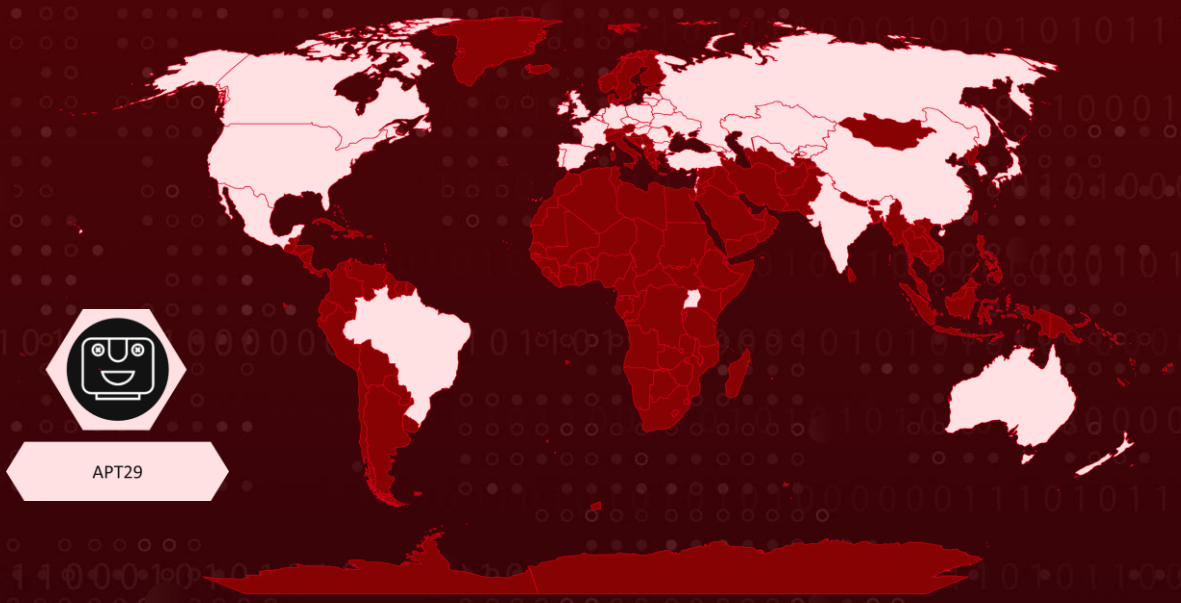
APT29 utilizes cloud storage service to deliver malicious payloads

Date of Publication	Admiralty code	TA Number
July 26, 2022	A1	TA2022155

Summary

APT29, a cyber espionage gang uses cloud storage services such as Google Drive and Dropbox to distribute malware to compromised systems. The gang used a phishing campaign that targeted several Western diplomatic missions and embassies in Portugal and Brazil.

Actor Map



Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**T1588** Obtain Capabilities	**T1588.002** Tool	**TA0001** Initial Access
T1566 Phishing	**T1566.001** Spearphishing Attachment	**TA0003** Execution	**T1059** Command and Scripting Interpreter
TA0003 Persistence	**T1547** Boot or Logon Autostart Execution	**T1547.001** Registry Run Keys / Startup Folder	**T1574** Hijack Execution Flow
T1574.002 DLL Side-Loading	**TA0005** Defense Evasion	**T1140** Deobfuscate/Decode Files or Information	**T1553** Subvert Trust Controls
T1553.005 Mark-of-the-Web Bypass	**T1027** Obfuscated Files or Information	**T1564** Hide Artifacts	**T1564.001** Hidden Files and Directories
TA0007 Discovery	**T1082** System Information Discovery	**T1016** System Network Configuration Discovery	**T1057** Process Discovery
TA0011 Command and Control	**T1071** Application Layer Protocol	**T1102** Web Service	**T1105** Ingress Tool Transfer
TA0010 Exfiltration	**T1567** Exfiltration Over Web Service	**T1567.002** Exfiltration to Cloud Storage	

Technical Details

#1

In May 2022, the Advanced Persistent Threat 29, also known as Cloaked Ursa, Cozy Duke, Nobelium, or Cozy Bear, was observed using web services as a communication vector for Command and Control integrating DropBox services in their malware campaigns for the first time. The actors' strategies continue to evolve, with recent campaigns incorporating popular online storage services such as Google Drive

#2

The phishing documents included a link to a malicious HTML file called EnvyScout, which functioned as a dropper for other malicious files in the target network, including a Cobalt Strike payload. EnvyScout dropper is an HTML file with embedded JavaScript that decodes and drops the next-stage payload.

#3

When the HTML file is executed, the JavaScript code decodes a bytes array and saves the result in the Download directory containing the signed software, relative DLLs, and the lure PDF named as Agenda.pdf.

#4

The omnipresent nature of cloud storage services, combined with the trust that millions of customers worldwide have in them, makes malware delivery significantly easier, and when combined with encryption, it becomes extremely difficult for organisations to detect malicious activity associated with the campaign.

Indicator of Compromise (IOC)

TYPE	VALUE
SHA256	CE9802B22A37AE26C02B1F2C3225955A7667495FCE5B106113434AB5A87AE28A F9B10323B120D8B12E72F74261E9E51A4780AC65F09967D7F4A4F4A8EABC6F4C A0BDD8A82103F045935C83CB2186524FF3FC2D1324907D9BD644EA5CEFACBAAF 347715F967DA5DEBFB01D3BA2EDE6922801C24988C8E6EA2541E370DED313C8B DE06CF27884440F51614A41623A4B84E0CB3082D6564EE352F6A4D8CF9D92EC5 0ED71B0F4F83590CCA66C0C9E9524A0C01D7A44CF06467C3AE588C1FE5B13118 CBE92ABB2E275770FDFF2E9187DEE07CCE1961B13C0EDA94237ACEEB06EEFBBD A018F4D5245FD775A17DC8437AD55C2F74FB6152DD4FDF16709A60DF2A063FFF 9230457E7B1AB614F0306E4AAAF08F1F79C11F897F635230AA4149CCFD090A3D FBA3A311A4C0A283753B5A0CDCADD3FE19F5A1174F03CB966F14D04BBF3D73EE 09F0EA9B239385EB22F794DCECAEC1273BE87F3F118A2DA067551778971CA677 56CFFE5E224ACBE5A7E19446238E5BB9110D9200B6B1EA8B552984D802B71547 295452A87C0FBB48EB87BE9DE061AB4E938194A3FE909D4BCB9BD6FF40B8B2F0 BC9AD574C42BC7B123BAAAFB3325CE2185E92E46979B2FAADDD4BC80DDFAC88A 761ED73512CB4392B98C84A34D3439240A73E389F09C2B4A8F0CCE6A212F529C 4C1ED0F6470D0BBE1CA4447981430E8CEB1157D818656BE9C8A992C56C10B541

TYPE	VALUE
URLs	porodicno[.]ba/wp-content/Agenda.html wethe6and9[.]ca/wp-content/Agenda.html dropbox[.]com/s/raw/dhueerinrg9k97k/agenda.html
Domains	crossfity[.]com techspaceinfo[.]com
IPV4	185.47.128[.]39 31.31.74[.]79
Registry Keys	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\AgendaE HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\AdobeUpdate
Email id	matysovi@seznam[.]cz

Actor Detail

NAME	ORIGIN	MOTIVE	TARGET LOCATIONs	TARGET INDUSTRIES
APT 29(Cozy Bear, The Dukes, Group 100, Yttrium, Iron Hemlock, Minidionis, CloudLook, ATK 7, ITG11, Grizzly Steppe, UNC2452, Dark Halo, SolarStorm, StellarParticle, Nobelium, Iron Ritual , Cloaked Ursa)	Russia	Information theft and espionage	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	Defense, Energy, Government, Law enforcement, Media, NGOs, Pharmaceutical, Telecommunications, Transportation, Think Tanks and Imagery.

References

https://unit42.paloaltonetworks.com/cloaked-ursa-online-storage-services-campaigns/

https://unit42.paloaltonetworks.com/atoms/cloaked-ursa/

What Next?

Book a free demo with **HivePro Uni5** to check your exposure to this advisory. HivePro Uni5 is a Threat Exposure Management Solution that proactively reduces an organization's attack surface before it gets exploited.

At Hive Pro we take a long hard look at your vulnerabilities so you can bolster your defenses and fine-tune your offensive cybersecurity tactics.

REPORT GENERATED ON

July 26, 2022 • 1:14 AM

More at www.hivepro.com