

# JUNE 5, 2024 MANDIANT ADVANTAGE THREAT INTELLIGENCE RELEASE

## New in this release

The Relevant Reporting sub-tabs under Threat Profiles Actor/Malware tabs are replaced with a top-level Reports tab, which shows higher quality report recommendations fed by an ML model.

Your Threat Profile
Customize Utils Korea

🚗 ACTORS

🎯 CAMPAIGNS

🐛 MALWARE

🛡️ VULNERABILITIES

📁 COLLECTIONS

OVERVIEW
MITRE ATT&CK

RELEVANT REPORTING

Report Title	Report Type	Associated Actors	Associated Malware	Published Date
Country Profile: North Korea (2023)	Country Profile	<span>🔗 APT37</span> , <span>🔗 APT43</span> , <span>🔗 UNC1069</span> , <span>🔗 UNC2970</span> , <span>🔗 UNC3782</span> , <span>🔗 UNC4736</span> , <span>🔗 UNC4899</span> , <span>🔗 UNC614</span>	<span>🔗 ASINCRAT</span> , <span>🔗 ATHARVAN</span> , <span>🔗 CABDRIVER</span> , <span>🔗 COUNTERLOOP</span> , <span>🔗 FASTVIEWER</span> , <span>🔗 FINEART</span> , <span>🔗 GIANTDIME</span> , <span>🔗 HAYBALE</span> , <span>🔗 LILITH</span> , <span>🔗 LOGCABIN</span> , <span>🔗 LONERUNNER</span> , <span>🔗 POWERHOUSE</span> , <span>🔗 QUARTZFIRE</span> , <span>🔗 QUINSTATUS</span> , <span>🔗 RUSTBUCKET</span> , <span>🔗 SHOWROOM</span> , <span>🔗 SIDESHOW</span> , <span>🔗 STONEBRIDGE</span> , <span>🔗 TALLCORAL</span> , <span>🔗 TOUCHMOVE</span> , <span>🔗 TOUCHSHIFT</span> , <span>🔗 TURKEYTROT</span> , <span>🔗 WHITEOUT</span> , <span>🔗 WHITESTORM</span>	March 27, 2024
Overview of China-Nexus Threats to OT	Trends and Forecasting	<span>🔗 APT1</span> , <span>🔗 APT10</span> , <span>🔗 APT12</span> , <span>🔗 APT19</span> , <span>🔗 APT22</span> , <span>🔗 APT24</span> , <span>🔗 APT27</span> , <span>🔗 APT40</span> , <span>🔗 APT41</span> , <span>🔗 APT5</span> , <span>🔗 TEMP.Hex</span> , <span>🔗 TEMP.Tick</span> , <span>🔗 UNC215</span> , <span>🔗 UNC2286</span> , <span>🔗 UNC251</span> , <span>🔗 UNC2743</span> , <span>🔗 UNC3236</span> , <span>🔗 UNC3569</span>	<span>🔗 BEACON</span> , <span>🔗 COLDLOCK</span> , <span>🔗 HYPERBRO</span> , <span>🔗 KEYPLUG</span> , <span>🔗 LOADINFO</span> , <span>🔗 NECKTIE</span> , <span>🔗 NIGHTSKY</span> , <span>🔗 PANDABOX</span> , <span>🔗 POISONPLUG</span> , <span>🔗 SICKMAN</span> , <span>🔗 SOGU</span> , <span>🔗 STEAMTRAIN</span>	February 8, 2024
Country Profile: China (2023)	Country Profile	<span>🔗 APT3</span> , <span>🔗 APT41</span> , <span>🔗 Conference Crew</span> , <span>🔗 TEMP.Hex</span> , <span>🔗 TEMP.Overboard</span> , <span>🔗 UNC2682</span> , <span>🔗 UNC302</span> , <span>🔗 UNC3236</span> , <span>🔗 UNC3569</span> , <span>🔗 UNC3886</span> , <span>🔗 UNC4191</span> , <span>🔗 UNC4528</span> , <span>🔗 UNC4713</span> , <span>🔗 UNC4841</span> , <span>🔗 UNC4936</span> , <span>🔗 UNC5007</span> , <span>🔗 UNC5089</span>	<span>🔗 BEACON</span> , <span>🔗 BIFROST</span> , <span>🔗 CHINACHOP</span> , <span>🔗 CKNIFE</span> , <span>🔗 DRIVERFRUIT</span> , <span>🔗 EIGHTFLY</span> , <span>🔗 EYEWELL</span> , <span>🔗 FAILPRINT</span> , <span>🔗 FLATSHHELL</span> , <span>🔗 LIGOLONG</span> , <span>🔗 LOCKBIT</span> , <span>🔗 MISTCLOAK</span> , <span>🔗 OCCULTBOX</span> , <span>🔗 OCCULTCOOP</span> , <span>🔗 OCCULTEGG</span> , <span>🔗 OCCULTYARD</span> , <span>🔗 OXEYE</span> , <span>🔗 QUICKFLOOD</span> , <span>🔗 REGEORG</span> , <span>🔗 SALTWATER</span> , <span>🔗 SEASIDE</span> , <span>🔗 SEASPRAY</span> , <span>🔗 SEASPY</span> , <span>🔗 SECRETSAUCE</span> , <span>🔗 SIDESTEP</span> , <span>🔗 SOGU</span> , <span>🔗 SOGU.SEC</span> , <span>🔗 SOLOSHIP</span> , <span>🔗 TRUTHTREE</span> , <span>🔗 VENUSTERRACE</span>	January 30, 2024
Strategic Perspective: 2023 Trends, 2024 Forecast	Executive Perspective	<span>🔗 UNC1530</span> , <span>🔗 UNC3840</span> , <span>🔗 UNC4736</span> , <span>🔗 UNC3886</span> , <span>🔗 APT43</span> , <span>🔗 TEMP.Hex</span> , <span>🔗 UNC2589</span> , <span>🔗 APT42</span> , <span>🔗 UNC2596</span> , <span>🔗 Sandworm Team</span> , <span>🔗 UNC3944</span> , <span>🔗 TEMP.Zagros</span> , <span>🔗 FIN11</span> , <span>🔗 UNC4841</span> , <span>🔗 UNC4191</span> , <span>🔗 UNC4221</span> , <span>🔗 UNC2448</span> , <span>🔗 UNC4528</span> , <span>🔗 APT29</span>	<span>🔗 MANGONUT</span> , <span>🔗 DARKBIT</span> , <span>🔗 V2</span> , <span>🔗 ALPHV</span> , <span>🔗 PLAYCRYPT</span> , <span>🔗 LOCKBIT</span> , <span>🔗 CONTI</span> , <span>🔗 TWOPIPE</span> , <span>🔗 WHIPWEAVE</span> , <span>🔗 COSMICENERGY</span> , <span>🔗 GOBRAT</span>	November 17, 2023
			<span>🔗 LOCKBIT</span> , <span>🔗 FORMBOOK</span> , <span>🔗 FONELAUNCH</span> , <span>🔗 MBR</span> , <span>🔗 GOOTLOADER</span> , <span>🔗 V2</span> , <span>🔗 MODESTM00N</span> , <span>🔗 ARGUEPATCH</span> , <span>🔗 PAPERDROR</span> , <span>🔗 MOTEISLAND</span> , <span>🔗 CADDYWIPER</span> , <span>🔗 ROYALLOCKER</span> , <span>🔗 BEACON</span>	

Before: Relevant Reporting as a sub-tab of Actors and Malware

**Your Threat Profile** ⚙️ Customize Utils Korea

🔒 Only you can see this information

👤 ACTORS
🎯 CAMPAIGNS
🐛 MALWARE
🛡️ VULNERABILITIES
📁 COLLECTIONS
📄 REPORTS

Report Title ↓	Report Type %	Associated Actors	Associated Malware	Last Updated %	Feedback
Country Profile: Russia (2023)	Country Profile	<span>🏠 APT28</span> <span>🏠 UNC3707</span> <span>🏠 UNC1543</span> <span>🏠 UNC4896</span> <span>🏠 Sandworm Team</span> <span>+ 7 MORE</span>	<span>🏠 ALPHV</span> <span>🏠 BEACON</span> <span>🏠 COSMICENERGY</span> <span>🏠 DRAHOBLAST</span> <span>🏠 HADES</span> <span>+ 10 MORE</span>	January 17, 2024	👍 🗨️
Country Profile: Saudi Arabia (2024)	Country Profile	---	---	February 29, 2024	👍 🗨️
Defensive Recommendations to Counter Threat Activities Observed Targeting Cloud Resources in Q3	Executive Perspective	---	---	February 13, 2024	👍 🗨️
Drivers of Cyber Espionage and Potential Lure Messages: March 2024	Trends and Forecasting	---	---	February 29, 2024	👍 🗨️
Iran-Nexus UNC1860 Targets Albania Electric Utility using OATBOAT and TOFULOAD Payload	Event Coverage/Implication	<span>🏠 UNC1860</span>	<span>🏠 LOWERASER</span> <span>🏠 OATBOAT</span> <span>🏠 OBFUSLAY</span> <span>🏠 SASHEYAWAY</span> <span>🏠 TOFULOAD</span> <span>+ 1 MORE</span>	February 29, 2024	👍 🗨️
OT Threat Activity Claimed in Underground Forums and Social Media Posts: December 2023	Event Coverage/Implication	---	---	January 4, 2024	👍 🗨️
Overview of North Korea-Nexus Threats to OT	Trends and Forecasting	<span>🏠 APT37</span> <span>🏠 UNC614</span>	<span>🏠 SHATTEREDGLASS</span> <span>🏠 BOOTWRECK</span> <span>🏠 MAUI</span> <span>🏠 RUHAPPY</span> <span>🏠 RYLK</span> <span>+ 6 MORE</span>	December 18, 2023	👍 🗨️
Overview of Russia-Nexus Threats to OT	Trends and Forecasting	<span>🏠 APT28</span>	---	January 4, 2024	👍 🗨️
UNC4399 Deploys SHARPCOFFEE.VBS to Ukrainian Energy Entities	Event Coverage/Implication	---	<span>🏠 SHARPCOFFEE</span>	December 11, 2023	👍 🗨️
2023 Review of New Malware and Tools Posing Heightened Risk to OT Environments	Trends and Forecasting	<span>🏠 Sandworm Team</span> <span>🏠 TEMP.Armageddon</span> <span>🏠 UNC4074</span> <span>🏠 UNC5203</span>	<span>🏠 BABYWIPER</span> <span>🏠 CHILLWIPE</span> <span>🏠 COOLWIPE</span> <span>🏠 COSMICENERGY</span> <span>🏠 COSMICENERGYLIGHTWORK</span> <span>+ 10 MORE</span>	February 16, 2024	👍 🗨️

Show 10 1 - 10 of 10 < 1 > Go to Page

After: Reports as a top-level tab