ThreatCure

Cyber Threat Advisory

Cyber Espionage Campaign "UNG0901"

CATEGORY

Malware Campaign

SEVERITY

High

Platforms

Windows

IMPACT

- Operational Disruption
- Financial Losses
- Data Exposure
- Security Control Evasion
- System Enumeration

Description

Cyber Espionage Campaign "UNG0901"

A sophisticated cyber espionage operation dubbed Operation CargoTalon has been observed targeting the Russian aerospace and defense sector, specifically the Voronezh Aircraft Production Association (VASO) a major aircraft manufacturer. The campaign is attributed to a threat actor cluster tracked as UNG0901 (Unknown Group 901).

The attackers use spear-phishing emails impersonating logistics or cargo delivery messages. These emails contain ZIP files disguised as official documents (notably товарно-транспортная накладная or Transport Consignment Notes, critical to Russian logistics). When the recipient opens the ZIP file, it contains a malicious LNK (shortcut) file.

Upon execution, the LNK uses **PowerShell** to execute a two-stage attack:

1. It displays a **decoy Excel document** to maintain user trust (often themed around Obltransterminal a sanctioned Russian terminal operator).

Indicator of Compromise

SHA-256

4d4304d7ad1a8d0dacb300739d4dcaade299b28f8be3f171628a7358720ca6c5

a8fdc27234b141a6bd7a6791aa9cb332654e47a57517142b3140ecf5b0683401

a9324a1fa529e5c115232cbbc60330d37cef5c20860bafc63b11e14d1e75697c

ae736c2b4886d75d5bbb86339fb034d37532c1fee2252193ea4acc4d75d8bfd7

b683235791e3106971269259026e05fdc2a4008f703ff2a4d32642877e57429a

c3caa439c255b5ccd87a336b7e3a90697832f548305c967c0c40d2dc40e2032e

e12f7ef9df1c42bc581a5f29105268f3759abea12c76f9cb4d145a8551064204

f6baa2b5e77e940fe54628f086926d08cc83c550cd2b4b34b4aab38fd79d2a0d

01f12bb3f4359fae1138a194237914f4fcdbf9e472804e428a765ad820f399be

02098f872d00cffabb21bd2a9aa3888d994a0003d3aa1c80adcfb43023809786

204544fc8a8cac64bb07825a7bd58c54cb3e605707e2d72206ac23a1657bfe1e

3e93c6cd9d31e0428085e620fdba017400e534f9b549d4041a5b0baaee4f7aff

413c9e2963b8cca256d3960285854614e2f2e78dba023713b3dd67af369d5d08

44ada9c8629d69dd3cf9662c521ee251876706ca3a169ca94c5421eb89e0d652

Indicator of Compromise

SHA-1

2a14a9dd1032479ab5bf8ed945ef9a22ebd4999d

4d8e20102ecbdced441c33a7be790e35e54c1b2d

c52d70b92e41db70d4ca342c8dc32eff7883c861

e84751baba286a352ee6e967eddf85bf07be1172

d9a4fd39a55cd20d55e00d3cace3f637b8888213

29a5e354ccbbef4671006138aa37dfe786bc6256

c77f71da23a274e5045788706acaf1d12d1bb4d7

89e20cf8e4d2bbcb59f4b0da8ecc38fb42a9537a

851157c01da6e85ffa94ded7f42cab19aa8528d6

c61a8f68a58461d386f443fb99346534ea7023d4

6942e07e7d08781cba571211a08e779838e72e9a

f5a45b498f41dd6ae56a37d6d577daedd1dc5f99

49a18dc1d8f84394d3373481dbac89d11e373dbd

1ba4c5a7749fa888cf4d9e60cff8e272b057a2f8

Indicator of Compromise

MD5

88453eb954669b5c7ac712ecf1e0179c
516827156014d123a050ed9c17afbeb8
08a92ba1d1d9e5c498dcaf53af7cd071
8cb7e417ae5418c4a1fec486a6e09046
b49a7ef89cfb317a540996c3425fcdc2
0599e9d6db2cd93f4e210dc746fa28ab
7442ace67cbf7095b46a025bfb25c497
40be360f4ed59777d6abb3d1b2f15b1f
be990a49fa1e3789ebc5c55961038029
d424a2d0a7481138ad219c98942cf628
7e52be17fd33a281c70fec14805113a8
59217400160c85d8e6e7e92511c382d3
65967d019076e700deb20dcbc989c99c
f807583c12e72746754b17cacc4626ff

Remediation

- Block .lnk and .zip attachments from unknown senders at the email gateway.
- Educate users on phishing campaigns that impersonate shipping/logistics firms.
- Monitor for PowerShell execution chains spawning from explorer.exe or shortcuts.
- Isolate suspicious endpoint behavior using EDR and quarantine if needed.
- Enable behavioral detection and ML policies in your EPP/EDR stack.
- Ensure endpoints use updated threat intelligence feeds and YARA detection (where supported).

THREAT CURE

RE-ARCHITECT YOUR THREAT LANDSCAPE

ThreatCure

Cyber Threat Advisory

Secure your byte world

Cyber Espionage Campaign "UNG0901"

Get Started Today

For more information about the ThreatCure ShieldOps Platform or to schedule a demo, please contact:

- Website: www.threatcure.net
- Email: info@threatcure.net