



Search...



FREE NEWSLETTER

Magazine Download Firewall Daily ▾ Essentials ▾ Knowledge Hub ▾ Features ▾ Business ▾ Events ▾ Advisory Board

TRENDING

TARGETED INDUSTRIES → IT & ITES | Government & LEA | Technology | Healthcare | BFSI

TARGETED COUNTRIES →

Home » Cyber News » Rogue RDP Files Used in Latest Campaign Targeting Ukrainian Government, Military

Rogue RDP Files Used in Latest Campaign Targeting Ukrainian Government, Military

Hackers are trying to gain remote access to Ukrainian government and military systems leveraging RDP files disguised as popular network and security services.

by Mihir Bagwe — October 23, 2024 Reading Time: 5 mins read



A Ukrainian mechanized infantry soldier fires at Opposing Forces (OPFOR) trying to advance forward, during the culminating force on force exercise of Combined Resolve XII at the Joint Multinational Readiness Center in Hohenfels, Germany Aug. 19, 2019. Combined Resolve is a biannual U.S. Army Europe and 7th Army Training Command-led exercise intended to evaluate and certify the readiness and interoperability of US forces mobilized to Europe in support of Atlantic Resolve. (U.S. Army photo by Sgt. Thomas Mort)

Share on LinkedIn

Share on Twitter



Follow Us On Google News

Hackers are trying to gain remote access to Ukrainian government and military systems leveraging Remote Desktop Protocol (RDP) configuration files, disguised as popular network and security services. Ukrainian cyber defenders say their investigation revealed meticulous planning that began in August and is aimed at a wider geography.

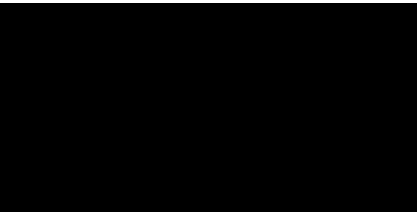
A new wave of malicious phishing emails targeted at key sectors in Ukraine has been observed by the Computer Emergency Response Team of Ukraine (CERT-UA). Hackers are attempting to exploit the Remote Desktop Protocol (RDP) to gain unauthorized access.

This campaign taps into the popularity of Amazon and Microsoft services, luring targets with promises of integration and the adoption of “Zero Trust Architecture” (ZTA). Attached to these phishing emails are RDP configuration files, and if opened, they allow attackers to connect to a remote server controlled by cybercriminals.

Attack Mechanism: Exploiting RDP Vulnerabilities

RDP is widely used for remote access in enterprise environments. However, in this attack, the “.rdp” files act as the entry point for the threat actors. Once the victim opens the file, it initiates an outbound connection to the attacker’s server.

“Taking into account the parameters of the RDP file, during such an RDP connection, the remote server was not only granted access to disks, network resources, printers, COM ports, audio devices, the clipboard and other resources on the local computer, but also allowed unauthorized running of third-party programs/scripts on the victim’s computer,” CERT-UA said.



Satnam Narang: W...



Partager

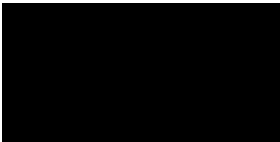
Latest Issue is Out. Subscribe Now

Latest Cyber News



Attack chain of the latest campaign (Source: CERT-UA)

This type of exploitation is possible on a machine that has improperly configured RDP settings. CERT-UA has noted that the attackers in this case are taking advantage of these misconfigurations to infiltrate networks, gain access to sensitive resources, and launch deeper attacks.



Also Read: [Ukrainian Government Agencies Hit by Stealthy MeshAgent Malware Campaign](#)

Global Implications

Though initially reported in Ukraine, CERT-UA has cautioned that this campaign’s infrastructure shows signs of a wider geographical footprint. The malicious activity dates back to August 2024, with domain names and IP addresses associated with these attacks pointing to preparations spanning multiple regions.

With attackers leveraging common themes like cloud services and zero-trust architecture, organizations worldwide could be at risk.

Strengthening Defenses Against Rogue RDP Files

Reducing the attack surface requires a multi-layered approach, particularly for organizations that rely on RDP for remote access. CERT-UA has issued several critical recommendations to help mitigate the risk of such attacks:

- **Block RDP Files:** Organizations should configure their mail gateways to block “rdp” files, preventing users from accidentally launching these malicious configurations.
- **Restrict RDP Access:** Firewalls should be adjusted to restrict RDP connections (specifically those initiated by mstsc.exe) to trusted internal resources, preventing unauthorized connections to external servers.
- **Set Group Policies:** Administrators should use group policies to disable resource redirection during RDP sessions, which attackers often exploit to access drives, printers, and other connected peripherals.

Also Read: [VectorStealer, Unlocking Doors to RDP Hijacking](#)

Additionally, CERT-UA advises security teams to scrutinize network logs for any suspicious connections on port 3389 (the default port for RDP traffic). Any unusual outbound connections should be flagged and investigated as potential indicators of compromise.

The activity has been assigned the identifier UAC-0215, suggesting it is part of a known campaign or actor group. Although the specific motivations behind these attacks are still unclear, the target selection—government agencies, industrial sectors, and military formations—implies a high degree of coordination, likely pointing to a nation-state or advanced persistent threat (APT) actor.

Below is a list of some Indicators of Compromise (IoCs) listed by CERT-UA:

File Hashes:

a5de73d69c1a7fbae2e71b98d48fe9b5
34c88cd591f73bc47a1a0fe2a4f594f628be98ad2366eeb4e467595115d8505a
Zero Trust Architecture Configuration.rdp

VULNERABILITIES

Cyble Warns of Escalating Cyber Risks in IoT and WordPress Plugins Amid Phishing Surge

🕒 NOVEMBER 4, 2024

CYBER NEWS

FBI Establishes 24/7 Command Post for Election Day Security Amid Cyber and Safety Concerns

🕒 NOVEMBER 4, 2024

FIREWALL DAILY

New Vulnerabilities in Fortinet, SonicWall, and Grafana Pose Significant Risks

🕒 NOVEMBER 4, 2024

CYBER NEWS

Ransomware Attack Disrupts Memorial Hospital’s EHR System, Temporarily Slows Operations

🕒 NOVEMBER 4, 2024

Categories

Select Category



Web Stories



Do This on Telegram, Yo...



If You Inst the iOS 18

	<div>8bcb741e204c25232a11a7084aa2221f</div> <div>07f185d9e341d549b198e60741e2c7f8d64dd2ca2c5d88d50b2c6ffcd3753810430b26b94a172fbf816e7d76</div> <div>ZTS Device Compatibility Test.rdp</div>
	<div>86f58115c891ce91b7364e5ff0314b31</div> <div>6e6680786fa5b023cf301b6bc5faaa89c86dc34b696f4b078cf22b1b353d5d3c</div> <div>Device Configuration Verification.rdp</div>
	<div>80b3cad4f70b6ea8924aa13d2730328b</div> <div>31f2cc1157248aec5135147073e49406d057bebf78b3361dd7cbb6e37708fbcc</div> <div>Zero Trust Architecture Configuration.rdp</div>
	<div>c0da30b71d58e071fc5863381444d9f0</div> <div>88fd6a36e8a61597dd71755b985e5fcd0b8308b69fc0f4b0fc7960fb80018622</div> <div>Device Security Requirements Check.rdp</div>
	<div>1595266bb78dc1e3d67f929154824c74</div> <div>b8327671ebc20db6f09efc4f19bd8c39d9e28c9a37bdd15b2fd62ade208d2e8a</div> <div>Device Security Requirements Check.rdp</div>
	<div>222c83d156a41735c38cc552a7084a86</div> <div>a5bbb109faefcecba695a84a737f5e47fa418cea39d654bb512a6f4a0b148758</div> <div>Device Configuration Verification.rdp</div>
	<div>fa9af43e9bbb55b7512b369084d91f4d</div> <div>5534cc837ba4fa3726322883449b3e97ca3e0d28c0ccf468b868397fdfa44e0b</div> <div>Zero Trust Architecture Configuration.rdp</div>
	<div>281a28800a4ba744bfde7b4aff46f24e</div> <div>b9ab481e7a9a92cfa2d53de8e7a3c75287cff6a3374f4202ec16ea9e03d80a0b</div> <div>Zero Trust Security Environment Compliance Check.rdp</div>
	<div>d37cd2c462af0e0643076b20c5ff561e</div> <div>18a078a976734c9ec562f5dfa3f5904ef5d37000fb8c1f5bd0dc2dee47203bf9</div> <div>Device Configuration Verification.rdp</div>
	<div>e465a4191a93195094a803e5d4703a90</div> <div>bb4d5a3f7a40c895882b73e1aca8c71ea40cef6c4f6732bec36e6342f6e2487a</div> <div>AWS IAM Quick Start.rdp</div>
	<div>3f753810430b26b94a172fbf816e7d76</div> <div>ef4bd88ec5e8b401594b22632fd05e401658cf78de681f81409eadf93f412ebd</div> <div>Device Configuration Verification.rdp</div>
	<div>434ffae8cfc3caa370be2e69ffaa95d1</div> <div>1cfe29f214d1177b66aec2b0d039fec47dd94c751fa95d34bc5da3bbab02213a</div> <div>Zero Trust Security Environment Compliance Check.rdp</div>
	<div>c287c05d91a19796b2649ebabd27394b</div> <div>3a2496db64507311f5fbd3aba0228b653f673fc2152a267a1386cbab33798db5</div> <div>ZTS Device Compatibility Test.rdp</div>
	<div>aabbfd1acd3f3a2212e348f2d6f169fc</div> <div>984082823dc1f122a1bb505700c25b27332f54942496814dfd0c68de0eba59dc</div> <div>AWS IAM Configuration.rdp</div>
	<div>b0a0ad4093e781a278541e4b01daa7a8</div> <div>383e63f40aecdd508e1790a8b7535e41b06b3f6984bb417218ca96e554b1164b</div> <div>Zero Trust Security Environment Compliance Check.rdp</div>
	<div>a18a1cad9df5b409963601c8e30669e4</div> <div>296d446cb2ad93255c45a2d4b674bbacb6d1581a94cf6bb5e54df5a742502680</div> <div>Device Security Requirements Check.rdp</div>
	<div>cbbc4903da831b6f1dc39d0c8d3fc413</div> <div>129ba064dfd9981575c00419ee9df1c7711679abc974fa4086076ebc3dc964f5</div> <div>ZTS Device Compatibility Test.rdp</div>
	<div>bd711dc427e17cc724f288cc5c3b0842</div> <div>f2acb92d0793d066e9414bc9e0369bd3ffa047b40720fe3bd3f2c0875d17a1cb</div> <div>AWS IAM Quick Start.rdp</div>
	<div>b38e7e8bba44bc5619b2689024ad9fca</div> <div>f357d26265a59e9c356be5a8ddb8d6533d1de222aae969c2ad4dc9c40863bfe8</div> <div>AWS IAM Compliance Check.rdp</div>

	406057b756096fa6b80f95334ba92034
	3fdffefc5a0af40c706377142fff718c7b87bc8b0daab10849f388d0
	AWS IAM Configuration.rdp
	db326d934e386059cc56c4e61695128e
	8b45f5a173e8e18b0d5c544f9221d7a1759847c28e62a25210ad8265f07e96d5
	Zero Trust Security Environment Compliance Check.rdp
	f58cf55b944f5942f1d120d95140b800
	ba4d58f2c5903776fe47c92a0ec3297cc7b9c8fa16b3bf5f40b46242e7092b46
	Zero Trust Security Environment Compliance Check.rdp

Source IPs:

37.153.155[.]143 (Email)
45.42.142[.]49 (Email)
45.42.142[.]89 (Email)
199.204.86[.]87 (Email)
181.215.148[.]194 (Email)
104.247.120[.]157 (Email)
204.111.198[.]27 (Email)
136.0.0[.]11 (Email)
38.180.110[.]238
179.43.148[.]82
45.11.230[.]105
45.141.58[.]60
95.217.113[.]133
185.187.155[.]74
141.195.117[.]125
185.76.79[.]178
2.58.201[.]112
89.46.234[.]115
84.32.188[.]193
38.180.146[.]210
84.32.188[.]197
45.80.193[.]9
45.67.85[.]40
45.134.111[.]123
84.32.188[.]153
62.72.7[.]213
93.188.163[.]16
23.160.56[.]122
95.156.207[.]121
84.32.188[.]148
166.0.187[.]233
185.216.72[.]196
38.180.146[.]230
84.32.188[.]200
45.11.231[.]8
162.252.175[.]233
13.49.21[.]253
179.43.163[.]18
46.19.141[.]186
193.29.59[.]9
135.181.130[.]232
45.134.110[.]83
185.187.155[.]73
23.160.56[.]100




Share this:



 More

Mihir Bagwe

Bagwe has nearly half a decade of experience in reporting on the latest cybersecurity news and trends, and interviewing cybersecurity subject matter experts. He has previously worked with ISMG and CISO MAG, publications focussed on addressing the cybersecurity needs of the C-Suite, particularly the CISO and CIO communities.



Subscribe to Daily News

Stay ahead of the curve with The Cyber Express's Daily News! Our newsletter delivers the latest cybersecurity headlines, expert insights, and critical updates straight to your inbox every morning. From breaking news and in-depth analysis to emerging threats and industry trends, our curated content ensures you’re always informed and prepared.

-  FACEBOOK
-  TWITTER
-  LINKEDIN

<div>About</div> <div>The Cyber Express</div> <div><i>#1 Trending Cybersecurity News and Magazine</i></div> <div>The Cyber Express is a handbook for all stakeholders of the internet that provides information security professionals with the latest news, updates and knowledge they need to combat cyber threats.</div>	<div>Contact</div> <div>For editorial queries: editor@thecyberexpress.com</div> <div>For marketing and Sales: raj@thecyberexpress.com</div> <div>For Events & Conferences related information: ashish.j@thecyberexpress.com</div> <div>Quick Links</div> <div><div>About Us</div><div>Contact Us</div><div>Editorial Calendar</div><div>Careers</div><div>The Cyber Express by Cyble Vulnerability Disclosure Policy</div><div>Cyble Trust Portal</div></div>	<div>Our Address</div> <div>We’re remote friendly, with office locations around the world:</div> <div>San Francisco, Atlanta, Rome, Dubai, Mumbai, Bangalore, Hyderabad, Singapore, Jakarta, Sydney, and Melbourne</div> <div>Headquarters:</div> <div>The Cyber Express LLC 555 North Point Center E Alpharetta, GA 30022, USA.</div> <div>India Office:</div> <div>Cyber Express Media Network HD-021, 4th Floor, C Wing, Building No.4. Nesco IT Park, WE Highway, Goregaon East, Mumbai, Maharashtra, India – 4000063</div>
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------