ADVISORY FOR ICM SECTOR

Earth Koshchei's Spear-Phishing Campaign

Original report published on: December 17, 2024[1]

Executive Summary

Trend Micro researchers have determined that Earth Koshchei (aka APT29 and Midnight Blizzard), a sophisticated cyber-espionage group, has launched a highly advanced Remote Desktop Protocol (RDP) attack campaign, integrating spear-phishing tactics and malicious RDP configuration files to compromise high-value targets.

The campaign primarily spreads through spear-phishing emails, tricking victims into opening malicious RDP files that establish connections to attacker-controlled RDP relays. These relays act as intermediaries and potentially lead to data leakage and malware installation, giving Earth Koshchei partial control over the compromised systems.

Background

Earth Koschei, allegedly linked to Russia's Foreign Intelligence Service (SVR) has a history of targeting diplomatic, military, energy, telecom, and IT companies in Western countries with the motivation believed to be primarily espionage. The group is known for adapting their TTPs and has deployed several techniques such as password spraying, brute forcing dormant accounts and watering hole attacks.

In this campaign, Earth Koschei utilised advanced red team tools, including Python Remote Desktop Protocol MITM tool (PyRDP), to intercept and manipulate RDP connections. This enables them to browse file systems, exfiltrate data, and execute malicious applications disguised as legitimate programs. The group's infrastructure consists of numerous proxy servers and rogue RDP backend servers, leveraging anonymisation services such as TOR, VPNs, and residential proxies to obscure their operations.

Detection and Mitigation

IMDA recommends organisations perform continual testing and validation of existing security controls to ensure detection and prevention identified in this advisory:

- Scan for Indicators of Compromise to detect threat actor activities (Annex A).
- Refer to the MITRE ATT&CK techniques (Annex B) in this advisory:
    - Create, test and validate detection rules against the threat behaviours.
    - Validate and deny/disable processes, ports and protocols that have no business need.
- Deploy a multi-layered protection solution that includes email sandboxing, domain URL filtering, endpoint detection and response protection, and network security measures to detect and block phishing attempts and other threats at various entry points.
- Adopt passwordless authentication such as FIDO2 passkeys and certificate-based authentication while ensuring robust protection of private keys.

- Conduct administration through secured intermediary devices with strong encryption such as jump hosts or Privileged Identity Management (PIM) tools.
- Disabled unused Remote Desktop Protocol (RDP) services, secure RDP access via VPNs, and monitor for suspicious activity.
- Detect and block the use of anonymisation layers such as TOR, residential proxies, or commercial VPNs.
- Deploy data loss prevention solution(s) to monitor that data remains within the enterprise or approved networks.
- Be alert for suspicious emails, particularly those containing phishing attempts or malicious attachment(s), and educate employees on social engineering tactics used by APTs.

IMDA encourages organisations to conduct thorough analyses to identify potential risks and assess their potential impact prior to deploying defensive measures.

Annex A - Indicators of Compromise

Malware Hash – SHA256	Remark
50bed47064e4ecd01c4a9271e63af7cfdf52ea4096f205470e41eef7eb01c1e1	RDP Configuration Files
648afcc709ac18c4fe235d24bf51a8230e9700b97c3dcc0a739816966f2b58b6	
280fbf353fdffefc5a0af40c706377142fff718c7b87bc8b0daab10849f388d0	
f357d26265a59e9c356be5a8ddb8d6533d1de222aae969c2ad4dc9c40863bfe8	
ba4d58f2c5903776fe47c92a0ec3297cc7b9c8fa16b3bf5f40b46242e7092b46	
8b45f5a173e8e18b0d5c544f9221d7a1759847c28e62a25210ad8265f07e96d5	
36e45fdeba3fdb3708fb1c2602c30cb5b66fbc5ea790f0716390d9f69c363542	
2fb1d01f9859c676ef37b060c5e8db0a12472c96260114a6edee45d8546184c9	
a246253fab152deac89b895a7c1bca76498b4aa044c907559c15109c1187a448	
1c1941b40718bf31ce190588beef9d941e217e6f64bd871f7aee921099a9d881	
f32fa0e3902a1f287280e2e6ddcbfe4fc0a47f1fa5ddb5e04a7651c51343621e	

IP Address	Remark
185[.]243[.]114[.]9	Host Rogue RDP Servers
5[.]187[.]49[.]186	
103[.]144[.]139[.]254	
185[.]177[.]126[.]225	
185[.]100[.]234[.]105	
45[.]137[.]21[.]10	
185[.]243[.]112[.]24	
185[.]243[.]115[.]124	
45[.]86[.]162[.]170	
46[.]30[.]189[.]91	
175[.]110[.]112[.]221	
92[.]204[.]164[.]50	
103[.]144[.]139[.]73	
103[.]144[.]139[.]74	

185[.]172[.]39[.]220	
5[.]183[.]95[.]158	
175[.]110[.]114[.]9	
46[.]30[.]189[.]62	
195[.]3[.]220[.]48	
46[.]30[.]188[.]187	
178[.]255[.]43[.]30	
104[.]161[.]58[.]10	
5[.]183[.]95[.]240	
37[.]28[.]153[.]214	
45[.]82[.]66[.]39	
103[.]144[.]139[.]253	
193[.]29[.]56[.]221	
162[.]216[.]243[.]210	
141[.]195[.]117[.]126	
141[.]195[.]117[.]127	
141[.]195[.]117[.]128	
141[.]195[.]117[.]129	
172[.]86[.]73[.]187	
155[.]138[.]238[.]169	
37[.]28[.]157[.]246	
185[.]187[.]155[.]69	
66[.]206[.]13[.]130	
185[.]172[.]39[.]230	
45[.]137[.]21[.]11	
45[.]11[.]230[.]105	RDP Relay
23[.]160[.]56[.]100	
45[.]141[.]58[.]60	
38[.]180[.]199[.]28	
45[.]134[.]110[.]83	
89[.]35[.]131[.]153	
185[.]76[.]79[.]244	
95[.]217[.]113[.]133	
185[.]187[.]155[.]74	
185[.]76[.]79[.]60	
141[.]195[.]117[.]125	
84[.]32[.]188[.]193	
38[.]180[.]146[.]210	
185[.]76[.]79[.]118	
2[.]58[.]201[.]112	
185[.]76[.]79[.]178	
38[.]180[.]146[.]193	
142[.]91[.]38[.]80	
84[.]32[.]188[.]197	
166[.]0[.]187[.]231	
89[.]46[.]234[.]115	

179[.]43[.]148[.]82	
178[.]239[.]171[.]41	
45[.]80[.]193[.]9	
179[.]43[.]180[.]74	
45[.]67[.]85[.]40	
5[.]133[.]9[.]252	
81[.]17[.]31[.]106	
38[.]180[.]90[.]36	
172[.]86[.]70[.]64	
185[.]76[.]79[.]130	
166[.]0[.]187[.]242	
151[.]236[.]16[.]149	
84[.]32[.]188[.]153	
185[.]187[.]155[.]81	
166[.]0[.]187[.]235	
45[.]134[.]111[.]123	
212[.]1[.]213[.]198	
151[.]236[.]16[.]220	
23[.]160[.]56[.]122	
166[.]0[.]187[.]243	
62[.]72[.]7[.]213	
151[.]236[.]16[.]226	
93[.]188[.]163[.]16	
2[.]58[.]203[.]61	
95[.]156[.]207[.]121	
185[.]216[.]72[.]196	
185[.]76[.]79[.]62	
162[.]252[.]172[.]167	
166[.]0[.]187[.]233	
84[.]32[.]188[.]148	
158[.]255[.]213[.]49	
38[.]180[.]146[.]230	
80[.]87[.]206[.]241	
158[.]255[.]213[.]227	
38[.]180[.]230[.]79	
37[.]1[.]196[.]172	
84[.]32[.]188[.]200	
109[.]205[.]214[.]50	
190[.]211[.]254[.]32	
109[.]205[.]214[.]45	
146[.]71[.]81[.]13	
185[.]187[.]155[.]33	
104[.]225[.]129[.]128	
109[.]205[.]214[.]52	
188[.]214[.]33[.]222	
93[.]188[.]164[.]74	

45[.]11[.]230[.]111	
23[.]160[.]56[.]105	
45[.]11[.]230[.]155	
45[.]11[.]231[.]9	
23[.]227[.]194[.]189	
166[.]0[.]187[.]236	
82[.]180[.]139[.]47	
23[.]160[.]56[.]110	
45[.]11[.]230[.]60	
38[.]180[.]83[.]120	
151[.]236[.]16[.]128	
158[.]255[.]213[.]185	
45[.]11[.]231[.]8	
23[.]108[.]190[.]249	
185[.]76[.]79[.]140	
178[.]162[.]203[.]91	
104[.]36[.]229[.]110	
166[.]0[.]187[.]241	
45[.]41[.]187[.]233	
23[.]160[.]56[.]115	
162[.]252[.]172[.]223	
149[.]154[.]158[.]205	
38[.]180[.]146[.]30	
151[.]236[.]16[.]236	
194[.]37[.]97[.]189	
151[.]236[.]16[.]98	
151[.]236[.]16[.]138	
166[.]0[.]187[.]245	
158[.]255[.]213[.]154	
162[.]252[.]175[.]233	
172[.]96[.]137[.]125	
212[.]1[.]213[.]200	
38[.]180[.]81[.]168	
185[.]187[.]155[.]72	
185[.]76[.]79[.]233	
38[.]180[.]146[.]216	
193[.]200[.]17[.]162	
2[.]58[.]200[.]78	
38[.]180[.]146[.]28	
151[.]236[.]16[.]24	
151[.]236[.]16[.]193	
151[.]236[.]16[.]22	
45[.]67[.]84[.]14	
162[.]252[.]172[.]158	
151[.]236[.]16[.]38	
198[.]50[.]106[.]140	

166[.]0[.]187[.]183	
2[.]58[.]201[.]27	
23[.]160[.]56[.]90	
149[.]154[.]158[.]250	
13[.]49[.]21[.]253	
45[.]134[.]111[.]126	
151[.]236[.]22[.]36	
38[.]180[.]88[.]106	
185[.]76[.]79[.]190	
38[.]180[.]146[.]32	
185[.]187[.]155[.]79	
162[.]252[.]172[.]155	
149[.]154[.]158[.]85	
89[.]46[.]234[.]152	
166[.]0[.]187[.]199	
185[.]76[.]79[.]167	
192[.]36[.]27[.]226	
185[.]187[.]155[.]78	
45[.]11[.]230[.]144	
23[.]160[.]56[.]123	
185[.]76[.]79[.]86	
38[.]180[.]5[.]60	
176[.]97[.]70[.]55	
166[.]0[.]187[.]252	
185[.]76[.]79[.]229	
185[.]76[.]79[.]59	
38[.]180[.]110[.]238	
45[.]134[.]110[.]78	
185[.]172[.]39[.]52	
198[.]50[.]106[.]141	
149[.]154[.]158[.]63	
185[.]216[.]72[.]192	
185[.]172[.]39[.]50	
2[.]58[.]200[.]79	
158[.]255[.]213[.]168	
45[.]141[.]58[.]59	
38[.]180[.]83[.]103	
89[.]46[.]234[.]93	
151[.]236[.]16[.]102	
158[.]255[.]213[.]192	
179[.]43[.]163[.]18	
46[.]19[.]141[.]186	
185[.]216[.]72[.]182	
192[.]121[.]23[.]126	
166[.]0[.]187[.]237	
209[.]182[.]225[.]10	

23[.]160[.]56[.]95	
38[.]180[.]137[.]213	
151[.]236[.]16[.]245	
2[.]58[.]200[.]80	
38[.]180[.]146[.]178	
38[.]180[.]91[.]2	
162[.]252[.]172[.]59	
185[.]187[.]155[.]71	
193[.]29[.]59[.]9	
151[.]236[.]15[.]134	
149[.]28[.]9[.]18	
45[.]134[.]110[.]82	
38[.]180[.]136[.]93	
135[.]181[.]130[.]232	
185[.]216[.]72[.]185	
2[.]58[.]14[.]80	
151[.]236[.]16[.]213	
45[.]134[.]110[.]55	
104[.]238[.]57[.]40	
162[.]252[.]172[.]109	
151[.]236[.]22[.]149	
192[.]36[.]57[.]107	
166[.]0[.]187[.]240	
45[.]137[.]213[.]17	
185[.]76[.]79[.]53	
185[.]76[.]79[.]16	
151[.]236[.]16[.]101	
104[.]238[.]60[.]216	
151[.]236[.]14[.]116	
185[.]172[.]39[.]51	
149[.]154[.]158[.]133	
38[.]180[.]146[.]29	
185[.]187[.]155[.]73	
46[.]249[.]38[.]131	

Domain	Remark
gov-au.cloud	RDP Relay
ua-mil[.]cloud	
mil-ee[.]cloud	
defence-au[.]cloud	
gov-aws[.]cloud	
gov-fi[.]cloud	
gov-gr[.]cloud	
gov-lt[.]cloud	
kam-lt[.]cloud	
mae-ro[.]cloud	

mfa-gov-tr[.]cloud	
aws-ukraine[.]cloud	
gov-ua[.]cloud	
govtr[.]cloud	
govua[.]cloud	
mfa-gov[.]cloud	
s3-army[.]cloud	
saiccloud[.]us	
ukrtelecom[.]cloud	
us-army[.]cloud	
us-mil[.]cloud	
awsplatform[.]online	
go-jp[.]cloud	
ua-gov[.]cloud	
gv-at[.]cloud	
s3-be[.]cloud	
ukrainesec[.]cloud	
amazonsolutions[.]cloud	
defense-gouv[.]cloud	
europa-eu[.]cloud	
gouv-fr[.]cloud	
mapn-ro[.]cloud	
mde-es[.]cloud	
mil-be[.]cloud	
mvep-hr[.]cloud	
s3-dk[.]cloud	
ua-sec[.]cloud	
dep-no[.]cloud	
difesa-it[.]cloud	
gov-pl[.]cloud	
morh-hr[.]cloud	
msz-pl[.]cloud	
quirinale[.]cloud	
mil-pl[.]cloud	
mzv-cz[.]cloud	
s3-nato[.]cloud	
gov-sk[.]cloud	
mzv-sk[.]cloud	
regeringskansliet-se[.]cloud	
s3-de[.]cloud	
ua-energy[.]cloud	
zixcorp[.]cloud	
bund-de[.]cloud	
mindef-nl[.]cloud	
presidencia-pt[.]cloud	
symbolsecurity[.]cloud	

trustifi[.]cloud	
s3-ua[.]cloud	
skykick[.]solutions	
softcat[.]cloud	
swcloud[.]us	
veeam[.]solutions	
shicloud[.]online	
s3-stig[.]cloud	
parseccomputer[.]cloud	
rrt[.]solutions	
rubrik[.]zone	
s3-proofpoint[.]cloud	
polycom[.]solutions	
pulsesecure[.]cloud	
s3-esa[.]cloud	
s3-rackspace[.]cloud	
servicenowinc[.]us	
aeinc[.]solutions	
capgemini[.]services	
mod-cloud[.]uk	
nrcc[.]cloud	
14-Mar	
s3-dnc[.]cloud	
s3-knowbe4[.]cloud	
s3-pt[.]cloud	
sipacolumbia[.]us	
brookings[.]cloud	
citoc[.]cloud	
clari[.]cloud	
justice[.]technology	
s3-aws[.]global	
s3-blackberry[.]cloud	
4freerussia[.]cloud	
democracyendowment[.]cloud	
gmfus[.]cloud	
mimecast[.]cloud	
stratfor[.]cloud	
barracuda[.]solutions	
caci[.]solutions	
druva[.]cloud	
exclaimer[.]solutions	
mil-pt[.]cloud	
oktacloud[.]us	
s3-atlassian[.]cloud	
s3-monitoring[.]cloud	
s3-us[.]navy	

s3-zoho[.]cloud	
usaid[.]cloud	
wrapsnet[.]cloud	
zoommeeting[.]zone	
albrightstonebridge[.]cloud	
backupify[.]cloud	
cer[.]zone	
crisisgroup[.]services	
forces-gc[.]cloud	
heritagecloud[.]org	
s3-acronis[.]cloud	
s3-bah[.]cloud	
s3-cloud[.]us	
s3-fbi[.]cloud	
s3-rand[.]cloud	
s3-ucia[.]cloud	
zero-trust[.]solutions	
amazonmeeting[.]cloud	
aspeninstitute[.]cloud	
c-r[.]services	
ceip[.]cloud	
cepa[.]solutions	
cnas[.]zone	
eopgov[.]cloud	
freedomhouse[.]cloud	
gc-cloud[.]ca	
googlemeet[.]zone	
macfound[.]services	
microsoft-meeting[.]cloud	
prio[.]zone	
admin-ch[.]cloud	
americanprogress[.]cloud	
csbaonline[.]cloud	
s3-csis[.]cloud	
s3-dgap[.]cloud	
s3-ida[.]cloud	
s3-iri[.]cloud	
s3-state[.]cloud	
ua-aws[.]army	
usip[.]us	
asucloud[.]us	
clearancejobs[.]cloud	
cwinc[.]cloud	
europeanvalues[.]cloud	
google-meet[.]cloud	
microsoftmeeting[.]cloud	

s3-hudson[.]cloud	
s3-marcus[.]cloud	
s3-ned[.]cloud	
s3-spacex[.]cloud	
statecloud[.]us	
foreignpolicy[.]cloud	
mfa-gov-il[.]cloud	
mod-gov-il[.]cloud	
ms-meetings[.]online	
ncfta[.]cloud	
ncsc[.]solutions	
ndu[.]solutions	
opensocietyfoundations[.]cloud	
s3-aws[.]cloud	
s3[.]army	
wilsoncenter[.]cloud	
zoommeeting[.]today	
ecfr[.]cloud	
go-meet-up[.]com	
zoom-meeting[.]live	
aws-meet[.]cloud	
awsmeet[.]cloud	
go-conference[.]cloud	
go-meeting[.]online	
zoom-meeting[.]pro	
gov-lv[.]cloud	
aws-il[.]cloud	
awsmeetings[.]online	
cfr-aws[.]cloud	
go-meeting[.]cloud	
ms-conference[.]cloud	
ms-meeting[.]online	
zoom-meeting[.]cloud	
zoom-meeting[.]today	
zoom-meetings[.]cloud	
go-meet[.]pro	
ms-meeting[.]com	
msconferences[.]cloud	
aws-data[.]cloud	
aws-meetings[.]cloud	
aws-join[.]cloud	
gov-trust[.]cloud	
s3-nsa[.]cloud	
ssi-gouv-fr[.]cloud	
aws-online[.]cloud	
minbuza[.]cloud	

Annex B - MITRE ATT&CK Tactics and Techniques

Tactic	Technique ID	Technique
Initial Access	T1566.001	Phishing: Spearphishing Attachment
	T1078.003	Valid Accounts: Local Accounts
Execution	T1204	User Execution
Persistence	T1574	Hijack Execution Flow
Defence Evasion	T1562.001	Impair Defences: Disable or Modify Tools
	T1036	Masquerading
Credential Access	T1552.001	Unsecured Credentials: Credentials In Files
Discovery	T1083	File and Directory Discovery
	T1018	Remote System Discovery
	T1046	Network Service Discovery
Lateral Movement	T1570	Lateral Tool Transfer
	T1563.002	Remote Service Session Hijacking: RDP Hijacking
	T1021.001	Remote Services: Remote Desktop Protocol
Collection	T1005	Data from Local System
	T1560.003	Archive Collected Data: Archive via Custom Method
Command and Control	T1090	Proxy
	T1105	Ingress Tool Transfer
Exfiltration	T1041	Exfiltration Over C2 Channel
	T1204.002	User Execution: Malicious File

References

1. ^ “Earth Koshchei Coopts Red Team Tools in Complex RDP Attacks”