## Severity

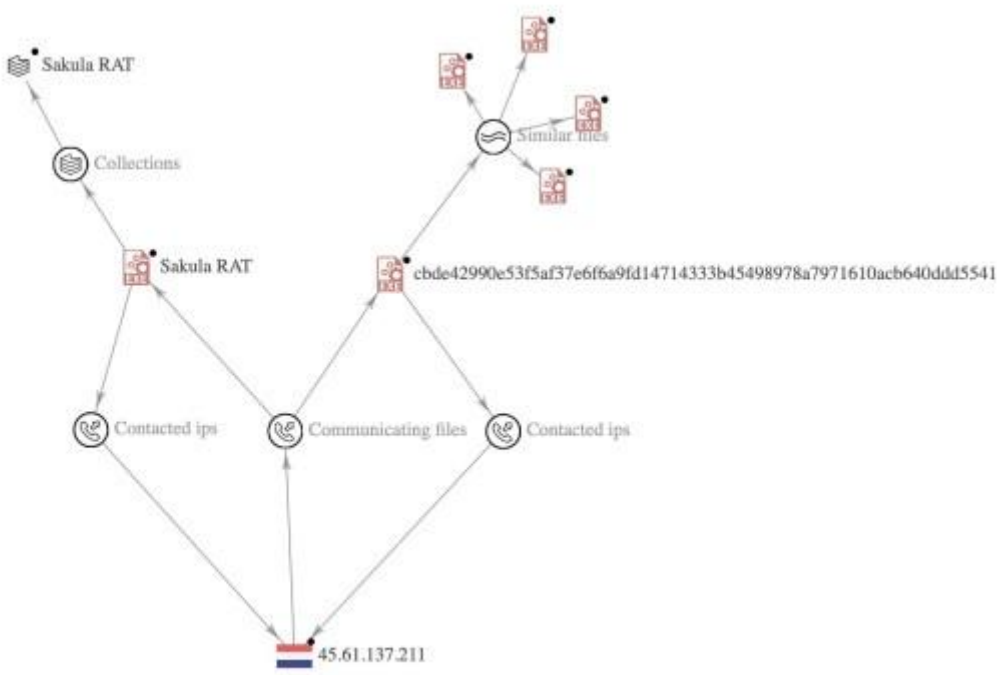
Medium

## Analysis Summary

Since the beginning of the Russian invasion of Ukraine, researchers have identified an undisclosed Advanced Persistent Threat (APT) group that is targeting Russian government organizations with at least four different spear-phishing campaigns. The threat actors intended to install a Remote Access Trojan (RAT) to take complete control of the affected PCs.

1. The first campaign involved attackers disseminating bespoke malware (named interactive_map_UA.exe) disguised as an interactive map of Ukraine.
2. In the second camapign the threat actor packed its custom malware in a tar archive entitled Patch_Log4j.tar.gz and disguised the malicious code as an update for the Log4j vulnerability. The staff of RT TV were the primary target of this campaign (which started in March).
3. In the third campaign, the Rostec defence conglomerate makes an appearance. The threat actor utilized the file name build_rosteh4.exe for its malware, ostensibly to make it appear like Rostec software.
4. The fourth campaign, which began in mid-April, employed a Word document with a phoney job advertisement for a “Strategy and Growth Analyst” position at Saudi Aramco, the Saudi Arabian public petroleum and natural gas company.

According to experts, these attacks might be done by Chinese-linked APT group.




The APT responsible for these activities is still being identified, however based on the infrastructure employed, with low confidence it is suspected that the group is a Chinese linked APT group. This is because all of the C2s are from BL Networks, which has previously been utilised by Chinese APTs. In addition, they detected infrastructure overlap between our malware and the Sakula Rat malware utilized by the Deep Panda APT.

## Impact

- Cyber Warfare
- Unauthorized Remote Access

## Indicators of Compromise

### Domain Name

- windowsipdate[.]com
- microsftupdetes[.]com
- mirror-exchange[.]com
- fatobara[.]com

### IP

- 168[.]100[.]11[.]142
- 192[.]153[.]57[.]83
- 45[.]61[.]137[.]211
- 206[.]188[.]197[.]35
- 91[.]210[.]104[.]54

### MD5

- bf9a9655ef18dc7010f472cededefbe6
- 671a2efbf69643e21ed3f0c0e1ae3fb0
- 52c794d252d9b4d22f5f4b51e878c469
- 31b8743bf033e28035174ebb78d6da74
- d28ee7c7cd9eb8d39b00e71907b235bd
- f93b93f7e210521053c5bc28e9e84437
- 9ec154c42bd173fc5625a926fbfb71cc
- 3eaffea946cb9e8cfe4b876cad2ce506
- 4e43c0ca1feebc1c7107a8ebb53255b9
- f3a2357ae9e0de9aef94b2f74e7a16f6
- 20071cde8a73faa92141c50183a671d4
- dac57710c999e39610537f0ce48edeae
- dd1faced42fbc7bc4ee6bbed467c7c80
- 35b7a4eeabac422758210f0d4d509f91
- c26575feb1456d079b391b8723fa826b
- 314c3739e66200581cbda125fccf5356
- ec481c83dc801b70f337a078b7edc71c
- 1715343c3925dc3d4d6486110e3dd6bd
- 0f47079fe6180aa494ab20744a96ae6f
- 5551730e5ebdd007619c3fb46ee73dc2
- 4d48b2af2da237608695f68b06f152fa
- 278fd8554ee06c6ce81ca9318889bdee
- 33dba43c177d68580b2324ef5d50c2d9
- f66f5e30daf15718f744183c29c6ae7c
- d04841bf168ca0ba4c96bff0a8be7871
- 705f95d64453bbb0012254fbfed24098
- 8c187b546c4500bf98efab94f6da3b07

### SHA-256

- cbde42990e53f5af37e6f6a9fd14714333b45498978a7971610acb640ddd5541
- 86ecd536c84cec6fc07c4cb3db63faa84f966a95763d855c7f6d7207d672911e
- 917820338751b08cefc635090fc23b4556fa77b9007a8f5d72c11e0453bfec95
- 22bdc42a86d3c70a01c51f20f5b7cfb353319691a8102f0fe3ea02af9079653e
- 12c20f9dbdb8955f3f88e28dc10241f35659dbcd74dadc9a10ca1b508722d69a
- 3f16055dc0f79f34f7644cae21dfe92ffc80f2c3839340a7beebd9436da5d0eb
- f5658588c36871421f287f12e7e9ba5afba783a7003da1043a9c52d10354b909
- ca95e8a8b6fb11b5129821f034b337b06cdf407fa9516619f3baed450ac1cf2d
- bac1790efe7618c5b2b9e34e6e1d36ec51592869bcc5fb304dd7554c32731093
- 5d039f4368f88a2299be91303c03143e340f700f1fc8aa0a8cdbfbc5a193c6be
- 4b622d63e6886b1430f6ca9cba519cbefde60cd8b6dbcade7c3a152c3930e7c7
- 0625566ec55f0a083d1c1a548a2631502f17e455066b29731e29d372918e6541
- 0925b3c05cef6d3476a97b7d4975e9e3ceefedf62f42663b9c02070e587b3f2d
- 111fef44ba63f11279572f1e7e4d6ce5613ef8fe3b76808355cdcbed47b49fec

- 1c886a9138f3b0e0b18f1c0da83719a9b5351db7ce24baa13c0e56ef65d96d02
- 1fb0cd76ec5ae70f08a87f9e81cb5e9b07f9b3306772ae723fa63ff5abfa0d07
- 27d19efedb6a7c8d3c65fe06fd5be9c3e236600e797e5058705db1e2335ec2ad
- 310fa9c65aa182a59e001e8f61c079e27d73b8eb5f8f8965509cb781d97ba811
- 3627b37b341efa0b36352d76480dce994f481e672ebf9fa2da114a1339cf6c01
- 3655420f72d0c14cfb113ccb53e9ac85b87883913c3844b3e0bfb7bd7230a9bd
- 3b2ef76ec2eb3b4db4b7efe14d88c5338f1dc4eb9a9cf309989362d193c25403
- 3e9254d8cb25b2abf4fb755feaaf41c0059c68067e64de01a9242e5d9e47ab33
- 3ff96e73aeb0419df67bc5fec786a4dc82e4a9051274b4fc3cbc3ae3af7fdf94
- 44118322165be32de86569972e9f599a3c79a2336ca6f76c29861b40905cd067
- 4b6b0c29ece1c4719ec4d5186fb6247603fa1f03bd473bf6ef6367995e8c1121
- 4f28db1131ace2fce96e84172e0a861eb471ea054799e1132eb4945e4dca550b
- 4f8c2079ac98a3e8e085be8e88ff7b53ea70cb131cba4bfd2784e391d24c27e9

SHA-1

- 7161345f02f04e4184a146f1f346bbfe34954ab0
- ccc1b7d15260b5f426af3b02bfdb321ff24c6992
- a1c1f0bfed2eeab60d5eb588c98a28d686b3f539
- 297cb386015cc62797917af1ab9082e5d3528801
- d6b267013d3a2183d773e0758e3ec4b40e8273bd
- 38a9f09c74355e2bcf74cf37456fffccf979b8fe
- 47604a9306f81d43423210123ffc5c8c5431ab09
- d78a7fd83e465feb701f3cc547544b7b95ddff37
- 4598321f83bea18dd42cccb018081e0d6c483e82
- 39a466a10658b05109187294f195c5db1cabb065
- c484a57d8d434bcb3f1838e249c6b8c564b639f3
- 447390819ddc843060f0fd61e2ef6fd2c9789877
- 66198757993f569b06ed47aa74e8a7ca3b09ceb1
- 584053510b183dac613222f80e09a7222de31ffb
- d012868dfa40791e4debb3a1dc80313888cdaf15
- 773565126edca75714bb7e53578bfc8de86c828e
- c6ee174a03982b83a54d6edfc00ecd84f849dcf8
- d9bc751ea000f68ae9c933d740dc8b4ffa916299
- ffc3c6058f3536447eed0248e74339fa60e11cb9
- b4d259d5b4a01a63d033ff022ee82a888fd367fd
- a2f9fc4d3f92135f5711c37f375b7da46daa36dc
- 90c8b22f546ade0cc3a273c4b239e22eb67f7bc0
- b011aa22e6e15a070567ff740b03871db5a7ae9b
- 10ec7517afd2392b22554f167dd733fa7b491197
- b1d8dbdbe97d775f1fd9eef9909e990fa440a723
- a4ce25c39a899b270ae9141caddd1d76f696484a
- 145fc78b2ef543941a0328c7f18ff36804750e33

## Remediation

- Look for IOCs in your surroundings.
- Disable all threat indicators at your respective controls.
- Never open links or attachments from unknown senders.
- Emails from unknown senders should always be treated with caution.
- Backup your data. Any damage in case of a successful attack will be mitigated if data is backed up.
- Maintain internet hygiene by updating your anti-virus software and downloading the latest patches.