KPMG Cyber Threat Intelligence Platform

DISGOMOJI - Evolving Techniques of Emoji Malware

DISGOMOJI malware, identified in 2024, is a sophisticated cyber espionage tool associated with the UTA0137 threat actor, believed to operate from Pakistan. Written in Golang for Linux systems, it utilizes Discord for C2 operations, employing emojis for communication. The malware primarily targets government entities, especially in India, aiming to exploit vulnerabilities and maintain persistent access, particularly on BOSS Linux systems.

The malware spreads via phishing emails or malicious downloads containing ZIP files with embedded UPX-packed ELF executables. Once executed, the ELF file downloads a lure documents (PDF and JPG) and retrieves DISGOMOJI payload from a remote server, storing it in a hidden directory in the user's home folder. Establishes persistence by adding cron jobs (@reboot) and manipulates XDG autostart entries for automatic startup. Establishes C2 using Discord, utilizing a custom tool named 'discord-c2'. Initially embeds hardcoded tokens and server IDs, but newer versions fetch them dynamically from attacker-controlled server. After establishing C2, DISGOMOJI sends a check-in message reporting victim information such as internal IP, username, hostname, operating system, and current working directory. Commands are received via Discord, using an emoji-based protocol (🕐 for processing, ✅ for completion) to execute specified tasks. The malware includes scripts to detect and copy files from connected USB devices, enhancing its data exfiltration capabilities. Newer variants prevent multiple instances and employ misleading strings and comments to evade detection. Post-infection, the malware utilizes tools like Nmap, Chisel, Ligolo, and oshi[.]at for network operations and data handling.

DISGOMOJI's Discord and emoji-based C2 operations showcase sophisticated espionage and data exfiltration methods, emphasizing the need for strong cybersecurity defenses.

What should you do?

- Monitor Indicators of Compromise (IoCs) in your environment to identify anomalies.
- Ensure your Windows environment is patched to the brim and is protected with multi-factor authentication.
- Conduct a comprehensive, full spectrum, threat assessment exercise to uncover blind spots and improvement areas.

The KPMG Cyber Threat Intelligence Platform is an industry defining, research-based capability for enhanced visibility into cyber threats.

Our machine ingestible feeds and analysis are the result of automated, sensor-based intelligence metrics with dedicated, expert insights of each threat to provide you the appropriate context on a timely basis in industry standard formats such as STIX/TAXII/MISP.

These feeds are additionally co-related with our industry partners and independent research for additional context. The intelligence obtained is then curated from strategic, tactical and operational perspective to give you a wide-ranging view of cyber threats.

We also assist you with our renowned cyber incident response and threat hunting services in case you identify an active threat in your environment.

We offer a wide-range of services, including:
Strategic threat intelligence report
Machine ingestible threat intelligence feeds
Threat intelligence driven pre-emptive threat hunting exercise
Cyber Incident Response Services

Contact us:

KPMG in India Cyber Response Hotline : +91 9176 471 471

Atul Gupta
Partner, Head of Cyber Security,
KPMG in India
T: +91 98100 81050
E: atulgupta@kpmg.com

B V, Raghavendra
Partner, KPMG in India
T: +91 98455 45202
E: raghavendrabv@kpmg.com

Sony Anthony
Partner, KPMG in India
T: +91 98455 65222
E: santhony@kpmg.com

Chandra Prakash
Partner, KPMG in India
T: +91 99000 20190
E: chandraprakash@kpmg.com

Manish Tembhurkar
Partner. KPMG in India
T: +91 98181 99432
E: mtembhurkar@kpmg.com

KPMG

KPMG Cyber Threat Intelligence Platform

DISGOMOJI - Evolving Techniques of Emoji Malware

Indicators of Compromise: IP Addresses
179.43.175[.]111

Indicators of Compromise: Domains	
esttsec[.]in	publicinfo[.]in
estbsec[.]in	epar-online[.]in
infosec2[.]in	emailnic[.]online
ordai[.]quest	parichay[.]online
secy-org[.]in	apsdelhicantt[.]in
nic-tech[.]in	awesindia[.]online
certdehli[.]in	defenseinsight[.]in
coordsec2[.]in	awesscholarship[.]in
admincoord[.]in	emailnic-tech[.]email
clawsindia[.]in	

Indicators of Compromise: Hashes
50fe93394528a0ede52f9eec6c1bf505
d5f2e3fafbb0701dc0f1adccc7141e63
2d4a5050c7ea6c83665807df151e067e
8bf9cf1363e404a9ad3e0fa9e53057cb
cd7067d58e2319ebc8ed0ecd6b61b2b6
52992eb3a59d7acb736cf9b607337d62
49cbbf586ba1480599be02915e5a8b34
de115e15a6689cf32519c3a046a78626
db0676733eb4ee2c490bdc4fe488b40f
da745b60b5ef5b4881c6bc4b7a48d784
13ee4bd10f05ee0499e18de68b3ea4d5
56cc70b66be99e01d354ba2aaf88041e
f68b17f1261aaa4460d759d95124fbd4
3d4e5dbf9b7a6e7336a354b71d4d1a8b
9821c180f81512f1b72c46e462fc759a
e6667ab32fbda86a2d2a72ed7e52b146
60fc5dc410b7482566a74d03549d8246

KPMG

KPMG Cyber Threat Intelligence Platform

DISGOMOJI - Evolving Techniques of Emoji Malware

Indicators of Compromise: Hashes
898bfd3df2ccd9508e0bfab672f5f61a
237961bbba6d4aa2e0fae720d4ece439
199c855998aedb0ce46e8d34c05eb0cb
e0102071722a87f119b12434ae651b48
635864ff270cf8e366a7747fb5996766
20b4eb5787faa00474f7d27c0fea1e4b
3ce8dfb3f1bff805cb6b85a9e950b3a2
01c34ccd7ca7c5cdf88272d8c9071004
501a6d48fd8f80a134cf71db3804cf95
f14e778f4d22df275c817ac3014873dc
c9969ece7bb47efac4b3b04cdc1538e5
56cb95b63162d0dfceb30100ded1131a
fc61b985d8c590860f397d943131bfb5
f2501e8b57486c427579eeda20b729fd
ee8d767069faf558886f1163a92e4009
9f3359ae571c247a8be28c0684678304
f5d8664cbf4a9e154d4a888e4384cb1d
a9182c812c7f7d3e505677a57c8a353b
55c90ff429e4fd72034922383aa31078
1443e58a298458c30ab91b37c0335bdadbacd756
0d4111ab5471c7f5b909bff336ba8cd66f9d8630
e5182d13d66c3efaa7676510581d622f98471895
3dff44bede709295fffd3ae3e9599f6ab8197af4
2dfe824d0298201e0efb30f16b3ce8a409ffe006
1c8cfa8f36897b6b1179dc4bce49b0e2f86e1a4e
31a1b6e836684c6d7b5d8f7a099dbe090282cbb0
789b41ddcee0166349cc106044932c76bfcb8cc0
765b17c1e2e1ab3d2fbdba3ccffcdcc4bd750102
465ef9d21e73493e9d531378756f91917f9567f4
8c969dbe0fe30244802cda1c8e33b04040831466
749a8d081e075b921436d07e323964da88bff609
e19c23d82d7e7e8e45b1d830ddc7ddb85087c4cc
c45e1cc5cd0c98388ec71221278950f9b1257ed8
d0aff8489c02230d4c0935e21125f81895bf6cde

KPMG

KPMG Cyber Threat Intelligence Platform

DISGOMOJI - Evolving Techniques of Emoji Malware

Indicators of Compromise: Hashes
25dc7c1237e5076c80fb867fb11d058387e1d154
c1916403a6ad05fed4da5fb53ce743b6ce49e0cb
5b7b0b0d7d59e616b0cf75a25ad67dfca89495c4
34cefe42aa8347c39a04eaca5a464fa35d6f1e62
caa130a8e3f5ca0a7f33de4b2b26e0e25dd10775
c1a80dd5be2de92a5a32d81a9fc146d4fd52ddb6
513b4b604d198f44041ed494ee8c7a7f94ac5038
88949119f88b15722a2b75ca84db7a6bfc822948
af137c7d1481e45217abd24a96f8aa2b416d294c
b8fd89cf6e9aae16321553a2e632e31b2cf2f057
892d434f3f59b3b8bd4ca500218a75d39c13ee5b
bcadcb345fc65a9c3d7c78566ad72a77c6076a11
4e2b14b18f5d68ce3dada1061526b03eafcd50b8
5dd201fa53cb5c76103579785a3d220d578dd12a
630530b11cbde6de840d7326152c1cb6bae06e0a
6f3f3c533a2b9031362d88bb7414bf332c93dc9d
7515a93da10b7d3f4619a38cc3f1a1bd25ddb847
038ae7e6e6708cb58db96512515177d84b71e8c2
bfdd02fa593d3858399da6bf591aeb10b2d1da40
c1c3454ed5bf32f22c855b19618bcd16e6549df8
e76c3f3a7158c16c28176053286dcb88ac646dbf
51a372fee89f885741515fa6fdf0ebce860f98145c9883f2e3e35c0fe4432885
d9f29a626857fa251393f056e454dfc02de53288ebe89a282bad38d03f614529
c981aa1f05adf030bacffc0e279cf9dc93cef877f7bce33ee27e9296363cf002
1e45d68106ca78f46be508427362b8ce24fdf5485c368f9369c913935cf04f99
38e1c0ca15ed83ed27148c31a31e0b33de627519ab2929d4aa69484534589086
5ecbc33fe3b345f2956cff566203e33b9390a3ed9923b990a46804880ae2f59b
cfb9ffb83877b421e95c9a2c3f65c106b9afb42babce7ba824671f9736bf0f7c
9709b0876c2a291cb57aa0646f9179d29d89abb2f8868663147ab0ca4e6c501b
1cdf1f32f31e226f037fda562985e481b7aa0b809971f2e40b713b034cf1d44e
1387b77a41e5a244c03ea7f5c90a2e528abe0ed7a4e6cb659183f7112c546046
26bf853b951e8d8ba6007e9d5c77f441faa739171e95f27f8d3851e07bc65b11
1e657d3047f3534dcd4539ce54db9f5901f7e53999bae340a850cc8d2aacc33c
fb30e5c67b92dc17d7a6e412f36d9b521842f8d7df38a00584c1362303b26655

KPMG

KPMG Cyber Threat Intelligence Platform

DISGOMOJI - Evolving Techniques of Emoji Malware

Indicators of Compromise: Hashes
582174441314665439790312 8fece87d7d9d71c4ade5fd40cdcf3cece2faf8f0
2abaae4f6794131108adf5b42e09ee5ce24769431a0e154feabe6052cfe70bf3
d3d5d0b210c3fc5c679419d6aa9014f62dcd60b0582cd8d544357f6420407b36
c177361992b207575b9aeb98aad7c2d522eace7ada6f1351434dd79a921ce260
bac7e6776c120b2b5da4d171afaea26144e77ad54f7516a0325260ee020b3f52
db91e23d9715464511057f2e15c9adc97d3f27fcfa308f05ac7e2de7275fdd32
4ddf0c70be0b81ab44f018521f788213de2ccf72b7a7f452f327b81172014182
207334927fc39278e37afe124769ed980e9a8ae86b0346408af64c86a7c99e6a
3d1b3ba5e1c1d1626595098f042913bc39601c80ab2c934cb994d3c053f218c5
0c284271e3d90a6673d84cf6291f92f32ade7c7f760bbe135880b949b38046ee
03666fb1c21d8a8cf38219691d2218d78eef5b00d20f26c25afde5d9e1daf80a
e89589e9ce043b28def17c91fa780322205ee08daa8b3cffe67b46bdae0e3a35
0cb88c8b8e2969af26678df4d3c395101c49c7c808d2cb2d7a0f00f60bdddcba
3845877017eb07be71820e8514502a3dcd24177540591c5ce2c13aca94caa4ac
af2201af8054e8e11eef7980fe15dc62eb2b7582f4f2bab4d8256f23f6db984e
db9afd2c59f20e04db37ddd38d1e911cdb4bddf39c24e4ce7cedda4eec984604
6c2f18f5d70f794b8826ee2575d973ddb07cbf9d15115973fe92df74079b6412
2cec6bd5e9ff046771623cfa0802cacd78b7521bf61b144e9c8dfa77d994927c
dfb72668791b4fe28884706b7756b02b951b43219e528b970ceb0369c86e3fd3
1b1d1d775571232235ed6fb84413eb60593340c1c1ea3b77bd72d3b68058f55c
76d9654f28bcaa713a99caa2839a572fc999a726827a0216da71ac184cee6d19
37bfa72c2820bcf9adb8707ae624452e0b769bc1c1f2a24ebb518c6e1794f3e2
8c8ef2d850bd9c987604e82571706e11612946122c6ab089bd54440c0113968e