Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

DISGOMOJI: Linux Malware Leveraging Emojis for C2

Date of Publication

June 18, 2024

Admiralty Code

A1

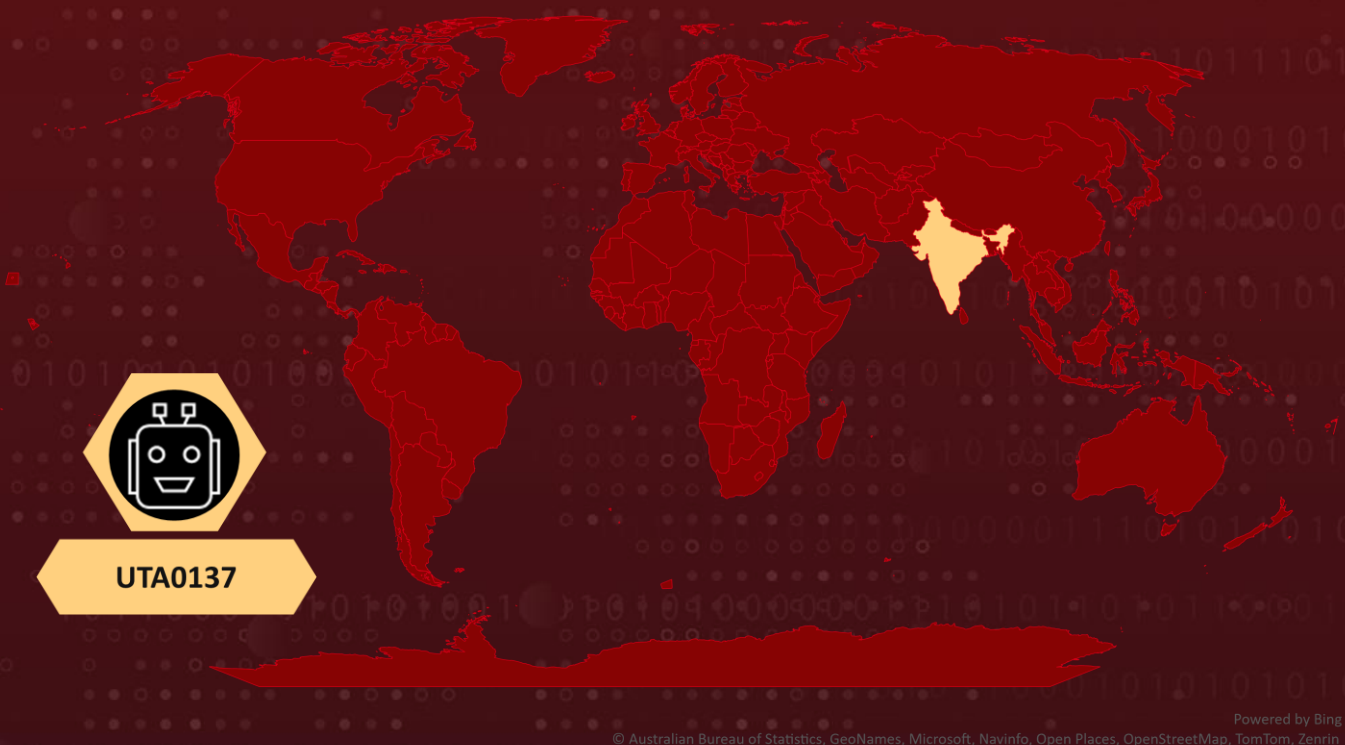
TA Number

TA2024232

Summary

Attack Discovered: 2024
Attack Region: India
Affected Industry: Government
Malware: DISGOMOJI
Actor: UTA0137
Attack: A newly discovered Linux malware, dubbed 'DISGOMOJI,' uses a novel approach by utilizing emojis to execute commands on infected devices. This malware has been targeting government agencies in India and is linked to a Pakistan-based threat actor known as UTA0137.

Attack Regions



Attack Details

#1 In 2024, a sophisticated cyber-espionage campaign attributed to the Pakistan-based threat actor UTA0137 has introduced a highly advanced malware known as DISGOMOJI. This malware, developed in Golang and specifically designed for Linux systems, is tailored to target Indian government entities. UTA0137's approach stands out due to its use of a customized version of the discord-c2 project, leveraging emojis and Discord for C2 operations—a method uncommonly seen in Linux-focused malware.

#2 DISGOMOJI is distributed as an UPX-packed ELF file bundled within a ZIP archive. Upon execution, it initiates by downloading a harmless lure file and subsequently retrieves a more malicious payload from a remote server hosted at clawsindia[.]in. To ensure persistence on infected systems, the malware installs an @reboot cron job and utilizes a monitoring script to copy files from connected USB devices for potential exfiltration.

#3 For communication and control, DISGOMOJI creates dedicated Discord channels named in a structured format, incorporating details such as the operating system type and victim username. It communicates covertly with its operators using an emoji-based protocol within Discord, allowing for discreet exchange of commands and data.

#4 UTA0137 has continuously enhanced DISGOMOJI's capabilities over time. Updates include the integration of features like the retrieval of lure documents and additional ELF files from servers, aimed at bolstering persistence and expanding functionality. These iterations also introduce mechanisms to prevent multiple instances of DISGOMOJI from running concurrently, dynamically manage authentication tokens for Discord communication, and employ obfuscation techniques to evade detection.

#5 The campaign orchestrated by UTA0137 underscores their expertise in cyber-espionage, blending sophisticated malware techniques with strategic utilization of legitimate platforms such as Discord for operational secrecy. Their toolkit encompasses a range of deception tools, penetration testing utilities, and the exploitation of vulnerabilities like DirtyPipe, showcasing a comprehensive approach to gathering intelligence.

#6 UTA0137's deployment of DISGOMOJI highlights the evolving nature of cyber threats, emphasizing the critical necessity for robust cybersecurity defenses across targeted organizations globally. Vigilance and proactive defense measures are crucial in mitigating such advanced and persistent threats in today's complex cybersecurity landscape.

Recommendations

Exercise Caution with Unsolicited Emails: Always exercise caution when receiving unexpected or urgent emails, especially those from unknown sources. Avoid downloading attachments from unsolicited emails to mitigate the risk of malware infections.

Robust Endpoint Security: Deploy advanced endpoint security solutions that include real-time malware detection and behavioral analysis. Regularly update antivirus and anti-malware software to ensure the latest threat definitions are in place. A multi-layered approach to endpoint security can prevent malwares from infiltrating the network through vulnerable endpoints and can detect and block malicious activities effectively.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0006 Credential Access	TA0007 Discovery	TA0010 Exfiltration	TA0011 Command and Control
T1566 Phishing	T1566.001 Spearphishing Attachment	T1053 Scheduled Task/Job	T1053.003 Cron
T1105 Ingress Tool Transfer	T1082 System Information Discovery	T1059 Command and Scripting Interpreter	T1071 Application Layer Protocol
T1027 Obfuscated Files or Information	T1027.002 Software Packing	T1547 Boot or Logon Autostart Execution	T1547.013 XDG Autostart Entries

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	5ecbc33fe3b345f2956cff566203e33b9390a3ed9923b990a46804880ae2f59b, cfb9ffb83877b421e95c9a2c3f65c106b9afb42babce7ba824671f9736bf0f7c, 51a372fee89f885741515fa6fdf0ebce860f98145c9883f2e3e35c0fe4432885, d9f29a626857fa251393f056e454dfc02de53288ebe89a282bad38d03f614529, 9709b0876c2a291cb57aa0646f9179d29d89abb2f8868663147ab0ca4e6c501b, 1cdf1f32f31e226f037fda562985e481b7aa0b809971f2e40b713b034cf1d44e, 1387b77a41e5a244c03ea7f5c90a2e528abe0ed7a4e6cb659183f7112c546046, 26bf853b951e8d8ba6007e9d5c77f441faa739171e95f27f8d3851e07bc65b11, 1e657d3047f3534dcd4539ce54db9f5901f7e53999bae340a850cc8d2aacc33c, fb30e5c67b92dc17d7a6e412f36d9b521842f8d7df38a00584c1362303b26655, 582174441314665439790312 8fece87d7d9d71c4ade5fd40cdcf3cece2faf8f0, 2abaae4f6794131108adf5b42e09ee5ce24769431a0e154feabe6052cfe70bf3, d3d5d0b210c3fc5c679419d6aa9014f62dcd60b0582cd8d544357f6420407b36, c177361992b207575b9aeb98aad7c2d522eace7ada6f1351434dd79a921ce260, bac7e6776c120b2b5da4d171afaea26144e77ad54f7516a0325260ee020b3f52, db91e23d9715464511057f2e15c9adc97d3f27fcfa308f05ac7e2de7275fdd32, 4ddf0c70be0b81ab44f018521f788213de2ccf72b7a7f452f327b81172014182, 207334927fc39278e37afe124769ed980e9a8ae86b0346408af64c86a7c99e6a, 3d1b3ba5e1c1d1626595098f042913bc39601c80ab2c934cb994d3c053f218c5, 0c284271e3d90a6673d84cf6291f92f32ade7c7f760bbe135880b949b38046ee, 03666fb1c21d8a8cf38219691d2218d78eef5b00d20f26c25afde5d9e1daf80a,

TYPE	VALUE
SHA256	e89589e9ce043b28def17c91fa780322205ee08daa8b3cffe67b46bdae0e3a35, 0cb88c8b8e2969af26678df4d3c395101c49c7c808d2cb2d7a0f00f60bdddcba, 3845877017eb07be71820e8514502a3dcd24177540591c5ce2c13aca94caa4ac, af2201af8054e8e11eef7980fe15dc62eb2b7582f4f2bab4d8256f23f6db984e, db9afd2c59f20e04db37ddd38d1e911cdb4bddf39c24e4ce7cedda4eec984604, 6c2f18f5d70f794b8826ee2575d973ddb07cbf9d15115973fe92df74079b6412, 2cec6bd5e9ff046771623cfa0802cacd78b7521bf61b144e9c8dfa77d994927c, dfb72668791b4fe28884706b7756b02b951b43219e528b970ceb0369c86e3fd3, 1b1d1d775571232235ed6fb84413eb60593340c1c1ea3b77bd72d3b68058f55c, 76d9654f28bcaa713a99caa2839a572fc999a726827a0216da71ac184cee6d19, 37bfa72c2820bcf9adb8707ae624452e0b769bc1c1f2a24ebb518c6e1794f3e2, c981aa1f05adf030bacffc0e279cf9dc93cef877f7bce33ee27e9296363cf002, 38e1c0ca15ed83ed27148c31a31e0b33de627519ab2929d4aa69484534589086, 8c8ef2d850bd9c987604e82571706e11612946122c6ab089bd54440c0113968e, ae59ba12ec6a42ee5b08c3e2ce91ec02071b2f5ad9338e3a19d690bd68acb860, 9c1ffafe0bb4388569fed2a8d4af591ce65ae00f47793ee97c07f686c5fab100, 1e45d68106ca78f46be508427362b8ce24fdf5485c368f9369c913935cf04f99, 0b5cf9bd917f0af03dd694ff4ce39b0b34a97c9f41b87feac1dc884a684f60ef, 98b24fb7aaaece7556aea2269b4e908dd79ff332ddaa5111caec49123840f364, 74e0af32c47e3bbe6becfb4027bbdcc01fbe36c92c70ce8edd676cc9aa3d6437, 1844156b1a72a7daa8de4139175a2bdeb4bd326b9e3e1fb4dd2ae00b313b0a44, fe7e7a5a1b1d634dec3fc9c6bc91c6e96ec635fece5af10cfac894fd228ca38d, ead993c1d537c239750e19a5700a58501dab319d5d271bf85137608448c1faa0, 5ef431a481c9baeb1d8cfaf6e1c323531a57c14a5b878575b267f2f969451fdb

TYPE	VALUE
Domain	admincoord[.]in, apsdelhicantt[.]in, awesindia[.]online, certdehli[.]in, clawsindia[.]in, coordsec2[.]in emailnic-tech[.]email, estbsec[.]in, outlook[.]emailnic[.]online, mail[.]defenseinsight[.]in, account[.]emailnic[.]online, webdisk[.]defenseinsight[.]in, m[.]emailnic[.]online, www[.]defenseinsight[.]in, login[.]emailnic[.]online, www[.]infosec2[.]in, esttsec[.]in, infosec2[.]in, cloud[.]publicinfo[.]in, publicinfo[.]in, email[.]publicinfo[.]in, ftp[.]publicinfo[.]in, www[.]publicinfo[.]in, _dc-mx[.]ae172f95f2ec[.]defenseinsight[.]in, insight[.]defenseinsight[.]in, www[.]emailnic[.]online, www[.]awesscholarship[.]in, ordai[.]quest, email[.]gov[.]in[.]parichay[.]online, email[.]parichay[.]online, emailnic[.]online, parichay[.]online, www[.]awesindia[.]online, www[.]certdehli[.]in, www[.]esttsec[.]in, www[.]ordai[.]quest, ww12[.]epar-online[.]in, accounts[.]emailnic[.]online, www[.]epar-online[.]in, play[.]emailnic[.]online, email[.]emailnic[.]online, email[.]emailnic-tech[.]email, epar[.]emailnic-tech[.]email, www[.]emailnic-tech[.]email, www[.]nic-tech[.]in, pcda[.]admincoord[.]in,

TYPE	VALUE
Domain	www[.]admincoord[.]in, email[.]apsdelhicantt[.]in, www[.]apsdelhicantt[.]in, smtp[.]mail[.]clawsindia[.]in, sql[.]clawsindia[.]in, test[.]clawsindia[.]in, webdisk[.]clawsindia[.]in, webmail[.]clawsindia[.]in, whm[.]clawsindia[.]in, dev[.]nic-tech[.]in, www[.]clawsindia[.]in, www[.]dev[.]clawsindia[.]in, mx10[.]clawsindia[.]in, mx4[.]clawsindia[.]in, ns1[.]clawsindia[.]in, old[.]clawsindia[.]in, pop[.]clawsindia[.]in, pop3[.]clawsindia[.]in, portal[.]clawsindia[.]in, shop[.]clawsindia[.]in, www[.]mailgate[.]clawsindia[.]in, www[.]old[.]clawsindia[.]in, www[.]shop[.]clawsindia[.]in, www[.]www[.]clawsindia[.]in, www2[.]clawsindia[.]in, defenseinsight[.]in, www[.]secy-org[.]in, awesscholarship[.]in, secy-org[.]in, nic-tech[.]in, epar-online[.]in, www[.]coordsec2[.]in, email[.]estbsec[.]in, email[.]coordsec2[.]in, adfs[.]clawsindia[.]in, app[.]clawsindia[.]in, autoconfig[.]clawsindia[.]in, blog[.]clawsindia[.]in, email[.]gov[.]in[.]estbsec[.]in, webdisk[.]estbsec[.]in, www[.]estbsec[.]in, localhost[.]clawsindia[.]in, m[.]clawsindia[.]in, mail[.]clawsindia[.]in, mail6[.]clawsindia[.]in, mailgate[.]clawsindia[.]in,

TYPE	VALUE
Domain	mailrelay[.]clawsindia[.]in, mbox[.]clawsindia[.]in, mx0[.]clawsindia[.]in, cpanel[.]clawsindia[.]in, dev[.]clawsindia[.]in, ftp[.]clawsindia[.]in, gate[.]clawsindia[.]in, help[.]clawsindia[.]in, imap[.]clawsindia[.]in, intranet[.]clawsindia[.]in, lists[.]clawsindia[.]in,
IPv4	3[.]111[.]168[.]95, 18[.]61[.]80[.]151, 179[.]43[.]175[.]111, 65[.]1[.]148[.]138, 15[.]206[.]164[.]242

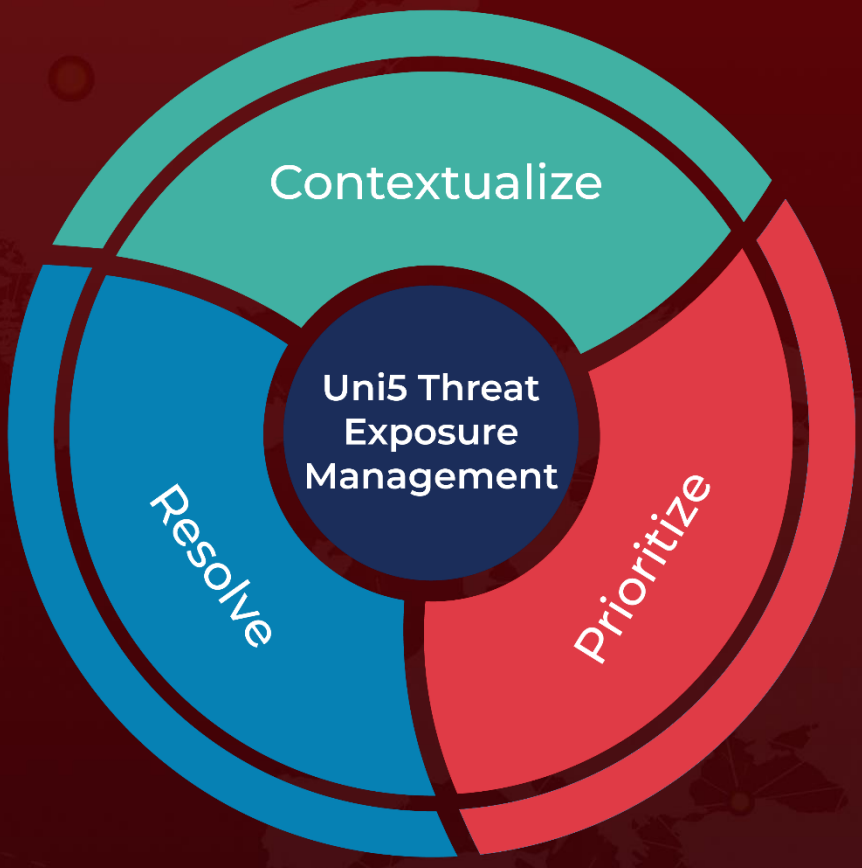
References

https://www.volexity.com/blog/2024/06/13/disgomoji-malware-used-to-target-indian-government/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

June 18, 2024 • 6:00 AM

More at www.hivepro.com