SECURITY ADVISORY

CYBER STASH

June, 2024

'DISGOMOJI': An Emojis Powered Malware

Context

A novel Linux malware, designated as 'DISGOMOJI,' has emerged, distinguished by its unconventional use of emojis to facilitate command execution on compromised systems. Predominantly directed at governmental entities within India, this malicious software has been linked to the activities of 'UTA0137,' a threat actor believed to operate out of Pakistan.

In functionality, DISGOMOJI exhibits traits akin to conventional backdoors and botnets, empowering threat actors with capabilities such as remote command execution, screen capturing, file exfiltration, payload deployment, and targeted file reconnaissance. However, its hallmark innovation resides in its adoption of Discord as a command and control (C2) platform, supplemented by emojis to issue directives. This departure from traditional text-based commands potentially augments its stealth capabilities, as it may elude detection by security solutions oriented towards scrutinizing text-based communications.

The emergence of DISGOMOJI underscores a notable evolution in malware tactics, where leveraging popular communication platforms and unconventional mediums like emojis represents a concerted effort to circumvent traditional cybersecurity defenses. As such, vigilance and adaptation in defensive strategies are imperative to counteract this emerging threat landscape effectively.

Mitigation

Defending against the 'DISGOMOJI' Malware Campaign necessitates more than just patching vulnerabilities. It involves actively limiting and monitoring adversary behaviours and conducting forensic-level post-breach analysis:

Forensic-Depth Memory Analysis: Incorporate regular memory-based forensic analysis across all systems into your threat hunting strategy to unveil malicious fileless executables

Blocking Network Traffic: Implement proactive network traffic blocking measures, including the restriction of suspicious IPs, domains, and connections from high-risk Autonomous System Numbers, Top-Level Domains, and countries.

User Security Awareness Training: Provide user awareness training to educate employees on the risks of opening attachments from unknown sources.

Technical Details

DISGOMOJI was initially uncovered encapsulated within a UPX-compressed ELF executable contained within a ZIP archive, a dissemination strategy commonly associated with phishing campaigns. While the malware exhibits a specific inclination towards the BOSS Linux distribution, it demonstrates adaptability to infiltrate various other Linux distributions as well.

Below are nine emojis utilized to signify commands for execution on an infected device:

Emojis	Command & Control
🏃	Execute a command on the device.
📸	Take a screenshot of the screen
👇	Download files from the victim's device and upload them to the command channel as attachments.
👈	Transfer a file from the compromised device to transfer[.]sh, a remote file-sharing service.
☝	Upload the file to the victim’s machine.
👉	Upload a file from the compromised device to Oshi (oshi[.]at), a remote file-storage service.
🔥	Search and retrieve files with extensions: CSV, DOC, ISO, JPG, ODP, ODS, ODT, PDF, PPT, RAR, SQL, TAR, XLS, and ZIP.
🦊	Collect all Mozilla Firefox profiles into a ZIP archive.
💀	Stop the malware process on the device.
🕐	Inform the attacker that the command is processing.
✅	Inform the attacker that the command has finished executing.

DISGOMOJI operates with a sophisticated methodology, primarily interacting through Discord channels where commands are initiated using emojis, a unique feature that distinguishes it from conventional malware. Upon receiving commands, indicated by specific emojis, DISGOMOJI responds with a "Clock" emoji to signify ongoing processing, replaced by a "Check Mark Button" emoji upon completion.

Initial Execution: Upon execution, the malware initiates by presenting a benign-looking PDF document, masquerading as an official beneficiary form from India's Defence Service Officer Provident Fund, to distract from its malicious activities. It proceeds to download and execute additional components, including the core DISGOMOJI malware and 'uevent_seqnum.sh,' a shell script integral to its operations.

Data Collection and Exfiltration: DISGOMOJI diligently collects crucial system details, such as IP address, username, hostname, operating system specifics, and current directory information, which it promptly forwards to the attackers' infrastructure. This data forms a critical part of the reconnaissance phase, aiding in subsequent malicious actions.

Command and Control: The malware leverages the discord-c2 open-source project to establish a clandestine communication channel via Discord servers. This platform facilitates command issuance through a specialized emoji protocol, where distinct emojis trigger varied functionalities tailored to the threat actors' objectives.

Persistence Mechanisms: To ensure persistence on compromised systems, DISGOMOJI employs multiple strategies. It creates a cron job configured with the @reboot directive, ensuring the malware initiates upon system startup. Additionally, alternative versions of DISGOMOJI utilize XDG AutoStart entries, bolstering its ability to persistently evade detection and removal attempts.

Payloads and Actions: Functionally, DISGOMOJI executes diverse commands dictated by its operators, encompassing screenshot capture, file theft, targeted file searches, and the deployment of supplementary payloads as dictated by operational requirements. Notably, the 'uevent_seqnum.sh' script enables the malware to scrutinize USB drives for exploitable data, further extending its reach beyond the primary system environment.

In totality, DISGOMOJI exemplifies a sophisticated blend of innovative command and control techniques, persistent infiltration methods, and multifaceted operational capabilities, underscoring its potential to effectively compromise and manipulate Linux-based systems within targeted environments.

Tactics, Techniques and Procedures

The notable TTPs related to the DISGOMOJI are:

T1566 - Phishing

DISGOMOJI employs phishing as its initial access vector, distributing malware through malicious email attachments. These attachments contain a ZIP archive containing a UPX-packed ELF executable, which executes upon user interaction.

T1102.002 - Web Service: Bidirectional Communication

To communicate with infected devices, DISGOMOJI uses Discord and emojis as a command and control (C2) channel. The malware connects to a Discord server where it listens for commands sent by the attacker via emojis. This unconventional method helps evade detection by security tools focusing on text-based C2 communications.

T1041 - Exfiltration Over C2 Channel

DISGOMOJI is designed to steal sensitive system and user data from infected devices. It gathers information such as IP addresses, usernames, hostnames, operating system details, and current working directories. This data is then exfiltrated to remote servers controlled by the attackers, facilitating espionage activities.

T1053.003 - Scheduled Task/Job: Cron:

To maintain persistence on compromised systems, DISGOMOJI utilizes cron jobs. It sets up cron jobs with the @reboot directive, ensuring that the malware automatically executes each time the system restarts.

Cyber Threat Intelligence

DISGOMOJI is attributed to UTA0137 based on Volexity's analysis. Operating from Pakistan, UTA0137 is known for cyber-espionage targeting Indian governmental bodies. CyberStash predicts DISGOMOJI's impact on non-governmental entities, critical infrastructure, and vulnerable sectors, signaling a shift to unconventional tactics with emojis in its C2, heightening risks across diverse targets.

Vigilance and strong defenses are crucial against these evolving threats. The innovative use of emojis in DISGOMOJI's command and control communications sets a precedent likely to inspire emulation among copycat adversaries. This trend could lead to the development of similar malware variants that adopt unconventional communication protocols to evade detection and amplify operational success.

References

Related IOC's & Yara Rules:

- https://github.com/volexity/threat-intel/blob/main/2024/2024-06-13%20DISGOMOJI/indicators/iocs.csv

Public Intelligence:

- https://www.bleepingcomputer.com/news/security/new-linux-malware-is-controlled-through-emojis-sent-from-discord/
- https://thehackernews.com/2024/06/pakistani-hackers-use-disgomoji-malware.html
- https://www.scmagazine.com/brief/emoji-controlled-malware-tapped-in-pakistan-linked-cyberespionage-campaign
- https://www.darkreading.com/remote-workforce/emojis-control-malware-discord-spy-campaign