Jun 19 2024

NETMANAGEIT

Intelligence Report

DISGOMOJI Malware Used to Target Indian Government

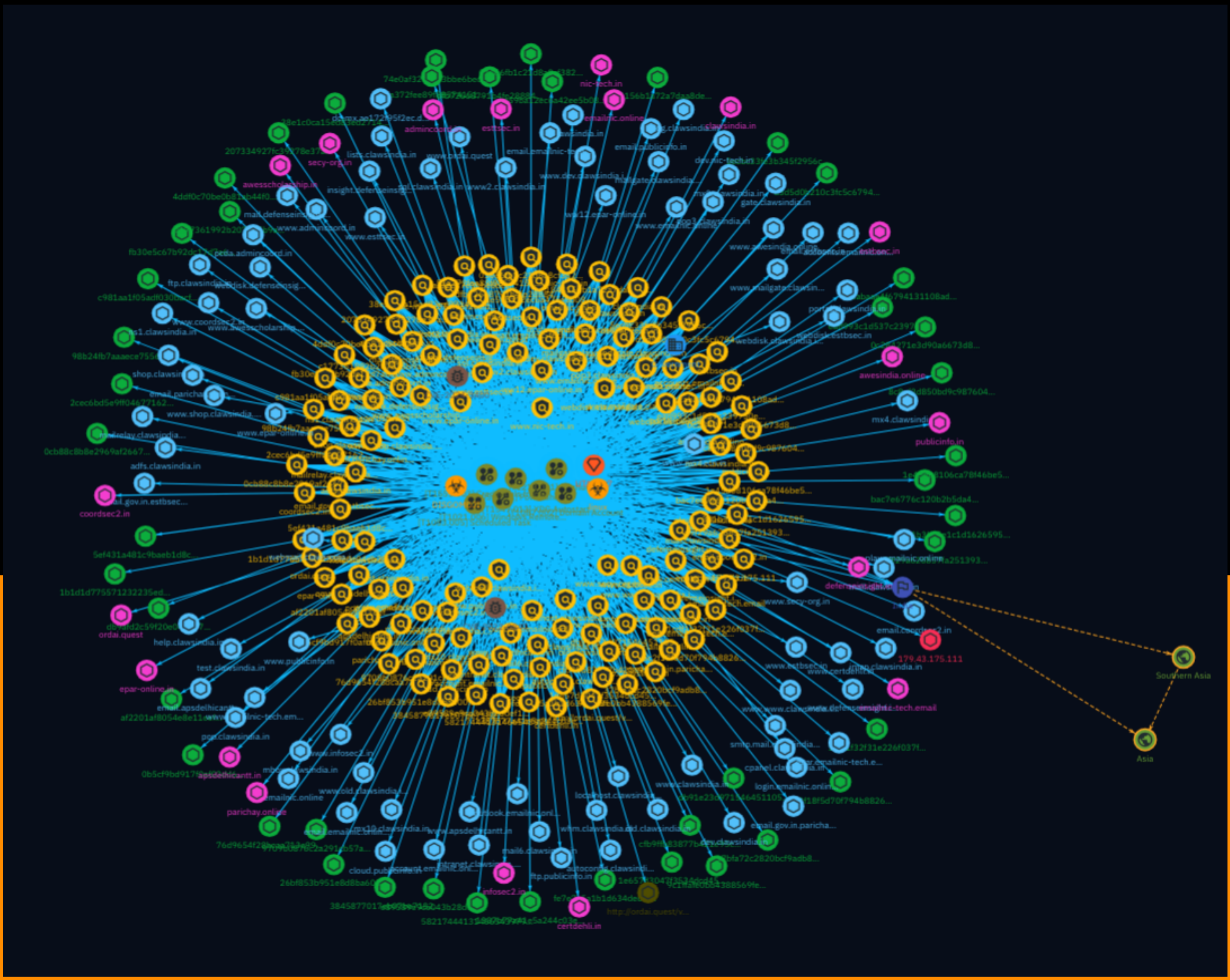

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Volexity identified a cyber-espionage campaign by a suspected Pakistan-based threat actor tracked as UTA0137 targeting government entities in India. The campaign leveraged the DISGOMOJI malware, a Golang-based Linux trojan that uses Discord for command and control via emojis. Key capabilities include data exfiltration, persistence mechanisms, and the ability to execute arbitrary commands. Volexity uncovered UTA0137's use of the DirtyPipe exploit against vulnerable BOSS Linux systems, as well as their post-exploitation tactics like network scanning and tunneling. The intrusions appear successful, highlighting UTA0137's evolving tradecraft and persistent interest in Indian targets.

Confidence

This value represents the confidence in the correctness of the data contained within this report.

100 / 100

Content

N/A

Attack-Pattern

Name
Domain Account
ID
T1087.002
Description
Adversaries may attempt to get a listing of domain accounts. This information can help adversaries determine which domain accounts exist to aid in follow-on behavior such as targeting specific accounts which possess particular privileges. Commands such as `net user /domain` and `net group /domain` of the [Net](https://attack.mitre.org/software/S0039) utility, `dscacheutil -q group`on macOS, and `ldapsearch` on Linux can list domain users and groups. [PowerShell](https://attack.mitre.org/techniques/T1059/001) cmdlets including `Get-ADUser` and `Get-ADGroupMember` may enumerate members of Active Directory groups.(Citation: CrowdStrike StellarParticle January 2022)
Name
Confluence
ID
T1213.001
Description

Adversaries may leverage Confluence repositories to mine valuable information. Often found in development environments alongside Atlassian JIRA, Confluence is generally used to store development-related documentation, however, in general may contain more diverse categories of useful information, such as: * Policies, procedures, and standards * Physical / logical network diagrams * System architecture diagrams * Technical system documentation * Testing / development credentials * Work / project schedules * Source code snippets * Links to network shares and other internal resources

Name

Credentials from Web Browsers

ID

T1555.003

Description

Adversaries may acquire credentials from web browsers by reading files specific to the target browser.(Citation: Talos Olympic Destroyer 2018) Web browsers commonly save credentials such as website usernames and passwords so that they do not need to be entered manually in the future. Web browsers typically store the credentials in an encrypted format within a credential store; however, methods exist to extract plaintext credentials from web browsers. For example, on Windows systems, encrypted credentials may be obtained from Google Chrome by reading a database file, `AppData\Local\Google\Chrome\User Data\Default\Login Data` and executing a SQL query: `SELECT action_url, username_value, password_value FROM logins;`. The plaintext password can then be obtained by passing the encrypted credentials to the Windows API function `CryptUnprotectData`, which uses the victim's cached logon credentials as the decryption key.(Citation: Microsoft CryptUnprotectData April 2018) Adversaries have executed similar procedures for common web browsers such as FireFox, Safari, Edge, etc.(Citation: Proofpoint Vega Credential Stealer May 2018)(Citation: FireEye HawkEye Malware July 2017) Windows stores Internet Explorer and Microsoft Edge credentials in Credential Lockers managed by the [Windows Credential Manager](https://attack.mitre.org/techniques/T1555/004). Adversaries may also acquire credentials by searching web browser process memory for patterns that commonly match credentials.(Citation: GitHub Mimikittenz July 2016) After acquiring credentials from web browsers, adversaries may attempt to recycle the credentials across different systems and/or accounts in order to expand access. This can result in significantly furthering an adversary's objective in cases

where credentials gained from web browsers overlap with privileged accounts (e.g. domain administrator).	

Name
Windows Remote Management
ID
T1021.006
Description
Adversaries may use [Valid Accounts](https://attack.mitre.org/techniques/T1078) to interact with remote systems using Windows Remote Management (WinRM). The adversary may then perform actions as the logged-on user. WinRM is the name of both a Windows service and a protocol that allows a user to interact with a remote system (e.g., run an executable, modify the Registry, modify services).(Citation: Microsoft WinRM) It may be called with the `winrm` command or by any number of programs such as PowerShell.(Citation: Jacobsen 2014) WinRM can be used as a method of remotely interacting with [Windows Management Instrumentation](https://attack.mitre.org/techniques/T1047).(Citation: MSDN WMI)
Name
XDG Autostart Entries
ID
T1547.013
Description
Adversaries may add or modify XDG Autostart Entries to execute malicious programs or commands when a user’s desktop environment is loaded at login. XDG Autostart entries are available for any XDG-compliant Linux system. XDG Autostart entries use Desktop Entry files (`.desktop`) to configure the user’s desktop environment upon user login. These configuration files determine what applications launch upon user login, define associated

applications to open specific file types, and define applications used to open removable media.(Citation: Free Desktop Application Autostart Feb 2006)(Citation: Free Desktop Entry Keys) Adversaries may abuse this feature to establish persistence by adding a path to a malicious binary or command to the `Exec` directive in the `.desktop` configuration file. When the user’s desktop environment is loaded at user login, the `.desktop` files located in the XDG Autostart directories are automatically executed. System-wide Autostart entries are located in the `/etc/xdg/autostart` directory while the user entries are located in the `~/.config/autostart` directory. Adversaries may combine this technique with [Masquerading](https://attack.mitre.org/techniques/T1036) to blend malicious Autostart entries with legitimate programs.(Citation: Red Canary Netwire Linux 2022)

Name

PowerShell

ID

T1059.001

Description

Adversaries may abuse PowerShell commands and scripts for execution. PowerShell is a powerful interactive command-line interface and scripting environment included in the Windows operating system.(Citation: TechNet PowerShell) Adversaries can use PowerShell to perform a number of actions, including discovery of information and execution of code. Examples include the `Start-Process` cmdlet which can be used to run an executable and the `Invoke-Command` cmdlet which runs a command locally or on a remote computer (though administrator permissions are required to use PowerShell to connect to remote systems). PowerShell may also be used to download and run executables from the Internet, which can be executed from disk or in memory without touching disk. A number of PowerShell-based offensive testing tools are available, including [Empire](https://attack.mitre.org/software/S0363), [PowerSploit](https://attack.mitre.org/software/S0194), [PoshC2](https://attack.mitre.org/software/S0378), and PSAttack.(Citation: Github PSAttack) PowerShell commands/scripts can also be executed without directly invoking the `powershell.exe` binary through interfaces to PowerShell's underlying `System.Management.Automation` assembly DLL exposed through the .NET framework and Windows Common Language Interface (CLI).(Citation: Sixdub PowerPick Jan 2016)(Citation: SilentBreak Offensive PS Dec 2015)(Citation: Microsoft PSfromCsharp APR 2014)

Name

Scheduled Task

ID

T1053.005

Description

Adversaries may abuse the Windows Task Scheduler to perform task scheduling for initial or recurring execution of malicious code. There are multiple ways to access the Task Scheduler in Windows. The [schtasks](https://attack.mitre.org/software/S0111) utility can be run directly on the command line, or the Task Scheduler can be opened through the GUI within the Administrator Tools section of the Control Panel. In some cases, adversaries have used a .NET wrapper for the Windows Task Scheduler, and alternatively, adversaries have used the Windows netapi32 library to create a scheduled task. The deprecated [at](https://attack.mitre.org/software/S0110) utility could also be abused by adversaries (ex: [At](https://attack.mitre.org/techniques/T1053/002)), though `at.exe` can not access tasks created with `schtasks` or the Control Panel. An adversary may use Windows Task Scheduler to execute programs at system startup or on a scheduled basis for persistence. The Windows Task Scheduler can also be abused to conduct remote Execution as part of Lateral Movement and/or to run a process under the context of a specified account (such as SYSTEM). Similar to [System Binary Proxy Execution](https://attack.mitre.org/techniques/T1218), adversaries have also abused the Windows Task Scheduler to potentially mask one-time execution under signed/trusted system processes.(Citation: ProofPoint Serpent) Adversaries may also create "hidden" scheduled tasks (i.e. [Hide Artifacts](https://attack.mitre.org/techniques/T1564)) that may not be visible to defender tools and manual queries used to enumerate tasks. Specifically, an adversary may hide a task from `schtasks /query` and the Task Scheduler by deleting the associated Security Descriptor (SD) registry value (where deletion of this value must be completed using SYSTEM permissions).(Citation: SigmaHQ)(Citation: Tarrask scheduled task) Adversaries may also employ alternate methods to hide tasks, such as altering the metadata (e.g., `Index` value) within associated registry keys.(Citation: Defending Against Scheduled Task Attacks in Windows Environments)

Domain-Name

Value
certdehli.in
nic-tech.in
apsdelhicantt.in
emailnic.online
secy-org.in
awesindia.online
clawsindia.in
epar-online.in
ordai.quest
estbsec.in
admincoord.in
publicinfo.in
esttsec.in

defenseinsight.in
parichay.online
emailnic-tech.email
infosec2.in
coordsec2.in
awesscholarship.in

StixFile

Value
ead993c1d537c239750e19a5700a58501dab319d5d271bf85137608448c1faa0
207334927fc39278e37afe124769ed980e9a8ae86b0346408af64c86a7c99e6a
3d1b3ba5e1c1d1626595098f042913bc39601c80ab2c934cb994d3c053f218c5
5ef431a481c9baeb1d8cfaf6e1c323531a57c14a5b878575b267f2f969451fdb
6c2f18f5d70f794b8826ee2575d973ddb07cbf9d15115973fe92df74079b6412
51a372fee89f885741515fa6fdf0ebce860f98145c9883f2e3e35c0fe4432885
8c8ef2d850bd9c987604e82571706e11612946122c6ab089bd54440c0113968e
1b1d1d775571232235ed6fb84413eb60593340c1c1ea3b77bd72d3b68058f55c
37bfa72c2820bcf9adb8707ae624452e0b769bc1c1f2a24ebb518c6e1794f3e2
5821744413146654397903128fece87d7d9d71c4ade5fd40cdcf3cece2faf8f0
03666fb1c21d8a8cf38219691d2218d78eef5b00d20f26c25afde5d9e1daf80a
5ecbc33fe3b345f2956cff566203e33b9390a3ed9923b990a46804880ae2f59b
e89589e9ce043b28def17c91fa780322205ee08daa8b3cffe67b46bdae0e3a35

c177361992b207575b9aeb98aad7c2d522eace7ada6f1351434dd79a921ce260
3845877017eb07be71820e8514502a3dcd24177540591c5ce2c13aca94caa4ac
38e1c0ca15ed83ed27148c31a31e0b33de627519ab2929d4aa69484534589086
76d9654f28bcaa713a99caa2839a572fc999a726827a0216da71ac184cee6d19
d3d5d0b210c3fc5c679419d6aa9014f62dcd60b0582cd8d544357f6420407b36
9709b0876c2a291cb57aa0646f9179d29d89abb2f8868663147ab0ca4e6c501b
1387b77a41e5a244c03ea7f5c90a2e528abe0ed7a4e6cb659183f7112c546046
2cec6bd5e9ff046771623cfa0802cacd78b7521bf61b144e9c8dfa77d994927c
0cb88c8b8e2969af26678df4d3c395101c49c7c808d2cb2d7a0f00f60bdddcba
bac7e6776c120b2b5da4d171afaea26144e77ad54f7516a0325260ee020b3f52
1e45d68106ca78f46be508427362b8ce24fdf5485c368f9369c913935cf04f99
1cdf1f32f31e226f037fda562985e481b7aa0b809971f2e40b713b034cf1d44e
af2201af8054e8e11eef7980fe15dc62eb2b7582f4f2bab4d8256f23f6db984e
98b24fb7aaaece7556aea2269b4e908dd79ff332ddaa5111caec49123840f364
fe7e7a5a1b1d634dec3fc9c6bc91c6e96ec635fece5af10cfac894fd228ca38d
0b5cf9bd917f0af03dd694ff4ce39b0b34a97c9f41b87feac1dc884a684f60ef
d9f29a626857fa251393f056e454dfc02de53288ebe89a282bad38d03f614529
9c1ffafe0bb4388569fed2a8d4af591ce65ae00f47793ee97c07f686c5fab100

0c284271e3d90a6673d84cf6291f92f32ade7c7f760bbe135880b949b38046ee

ae59ba12ec6a42ee5b08c3e2ce91ec02071b2f5ad9338e3a19d690bd68acb860

26bf853b951e8d8ba6007e9d5c77f441faa739171e95f27f8d3851e07bc65b11

dfb72668791b4fe28884706b7756b02b951b43219e528b970ceb0369c86e3fd3

cfb9ffb83877b421e95c9a2c3f65c106b9afb42babce7ba824671f9736bf0f7c

1e657d3047f3534dcd4539ce54db9f5901f7e53999bae340a850cc8d2aacc33c

fb30e5c67b92dc17d7a6e412f36d9b521842f8d7df38a00584c1362303b26655

c981aa1f05adf030bacffc0e279cf9dc93cef877f7bce33ee27e9296363cf002

db9afd2c59f20e04db37ddd38d1e911cdb4bddf39c24e4ce7cedda4eec984604

db91e23d9715464511057f2e15c9adc97d3f27fcfa308f05ac7e2de7275fdd32

2abaae4f6794131108adf5b42e09ee5ce24769431a0e154feabe6052cfe70bf3

74e0af32c47e3bbe6becfb4027bbdcc01fbe36c92c70ce8edd676cc9aa3d6437

4ddf0c70be0b81ab44f018521f788213de2ccf72b7a7f452f327b81172014182

1844156b1a72a7daa8de4139175a2bdeb4bd326b9e3e1fb4dd2ae00b313b0a44

Hostname

Value
dc-mx.ae172f95f2ec.defenseinsight.in
lists.clawsindia.in
www.emailnic.online
portal.clawsindia.in
autoconfig.clawsindia.in
dev.nic-tech.in
www.defenseinsight.in
old.clawsindia.in
email.parichay.online
email.coordsec2.in
email.emailnic-tech.email
webmail.clawsindia.in
imap.clawsindia.in

cloud.publicinfo.in
pop.clawsindia.in
www.certdehli.in
www.infosec2.in
epar.emailnic-tech.email
smtp.mail.clawsindia.in
mbox.clawsindia.in
www.mailgate.clawsindia.in
www.secy-org.in
dev.clawsindia.in
cpanel.clawsindia.in
m.emailnic.online
ns1.clawsindia.in
www.nic-tech.in
insight.defenseinsight.in
ww12.epar-online.in

External References

- https://raw.githubusercontent.com/volexity/threat-intel/main/2024/2024-06-13%20DISGOMOJI/indicators/iocs.csv
- https://www.volexity.com/blog/2024/06/13/disgomoji-malware-used-to-target-indian-government/
- https://otx.alienvault.com/pulse/66712446e23b1d14e4f293eb