

NETMANAGEIT

Intelligence Report

A novel backdoor tailored for covert access over the roaming exchange

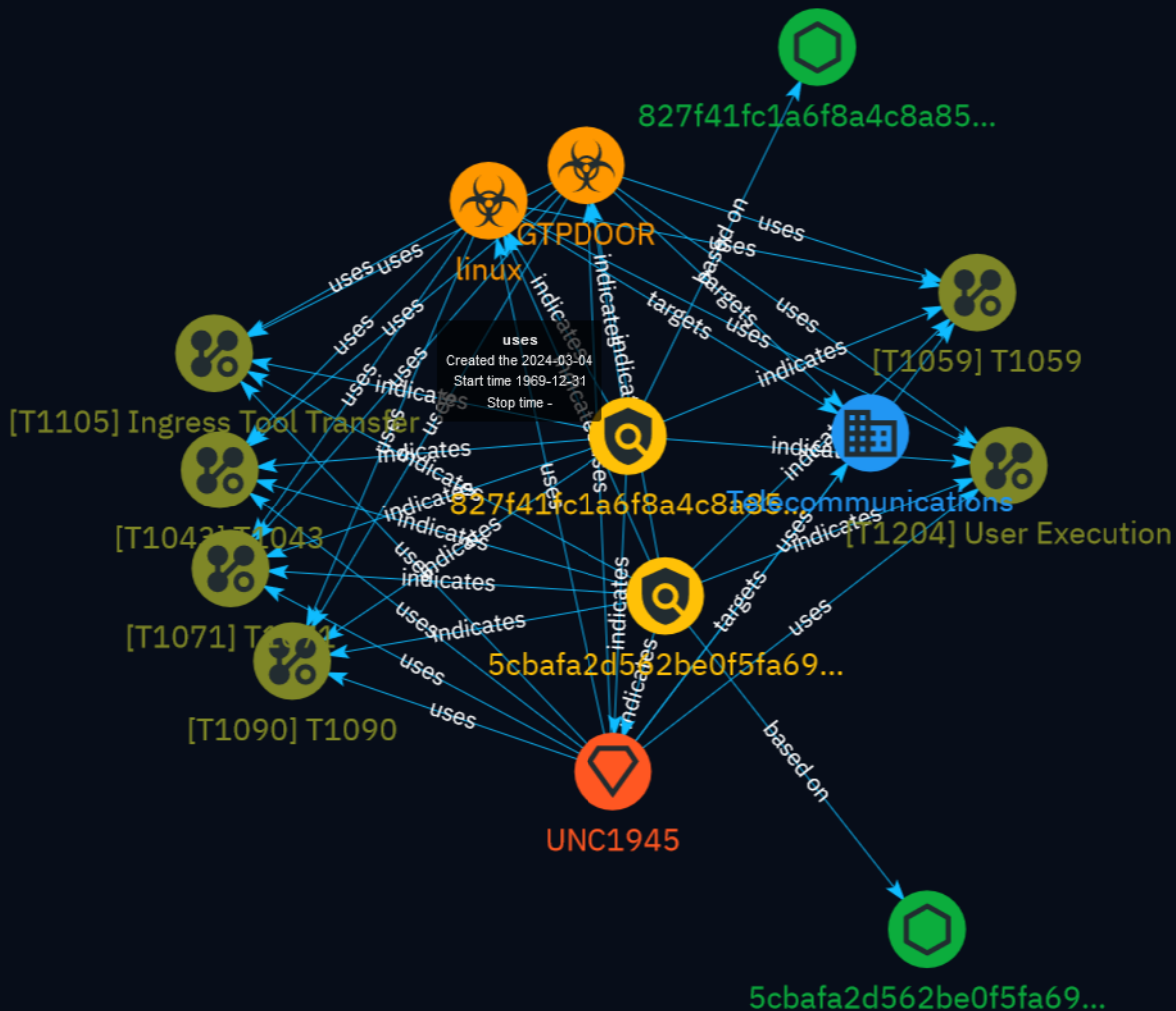


Table of contents

Overview

● Description	4
● Confidence	4
● Content	5

Entities

● Indicator	6
● Malware	7
● Intrusion-Set	8
● Attack-Pattern	9
● Sector	14

Observables

● StixFile	15
------------	----



External References

- External References

16

Overview

Description

GTPDOOR is Linux malware that communicates C2 traffic over GTP-C signalling messages, blending in with normal telco traffic. It can execute commands sent in GTP echo requests and probe hosts covertly via TCP packets. Versions target x86 and i386 architectures.

Confidence

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

100 / 100

Content

N/A

Indicator

Name

827f41fc1a6f8a4c8a8575b3e2349aeaba0dfc2c9390ef1cceeef1bb85c34161

Pattern Type

stix

Pattern

[file:hashes!'SHA-256' =
'827f41fc1a6f8a4c8a8575b3e2349aeaba0dfc2c9390ef1cceeef1bb85c34161']

Name

5cbafa2d562be0f5fa690f8d551cdb0bee9fc299959b749b99d44ae3fda782e4

Pattern Type

stix

Pattern

[file:hashes!'SHA-256' =
'5cbafa2d562be0f5fa690f8d551cdb0bee9fc299959b749b99d44ae3fda782e4']

Malware

Name

GTPDOOR

Name

linux

Intrusion-Set

Name

UNC1945

Attack-Pattern

Name

T1043

ID

T1043

Description

This technique has been deprecated. Please use [Non-Standard Port](https://attack.mitre.org/techniques/T1571) where appropriate. Adversaries may communicate over a commonly used port to bypass firewalls or network detection systems and to blend with normal network activity to avoid more detailed inspection. They may use commonly open ports such as * TCP:80 (HTTP) * TCP:443 (HTTPS) * TCP:25 (SMTP) * TCP/UDP:53 (DNS) They may use the protocol associated with the port or a completely different protocol. For connections that occur internally within an enclave (such as those between a proxy or pivot node and other nodes), examples of common ports are * TCP/UDP:135 (RPC) * TCP/UDP:22 (SSH) * TCP/UDP:3389 (RDP)

Name

T1059

ID

T1059

Description

Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of [Unix Shell](<https://attack.mitre.org/techniques/T1059/004>) while Windows installations include the [Windows Command Shell](<https://attack.mitre.org/techniques/T1059/003>) and [PowerShell](<https://attack.mitre.org/techniques/T1059/001>). There are also cross-platform interpreters such as [Python](<https://attack.mitre.org/techniques/T1059/006>), as well as those commonly associated with client applications such as [JavaScript](<https://attack.mitre.org/techniques/T1059/007>) and [Visual Basic](<https://attack.mitre.org/techniques/T1059/005>). Adversaries may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in [Initial Access](<https://attack.mitre.org/tactics/TA0001>) payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells, as well as utilize various [Remote Services](<https://attack.mitre.org/techniques/T1021>) in order to achieve remote Execution. (Citation: Powershell Remote Commands)(Citation: Cisco IOS Software Integrity Assurance - Command History)(Citation: Remote Shell Execution in Python)

Name

T1090

ID

T1090

Description

Adversaries may use a connection proxy to direct network traffic between systems or act as an intermediary for network communications to a command and control server to avoid direct connections to their infrastructure. Many tools exist that enable traffic redirection through proxies or port redirection, including [HTRAN](<https://attack.mitre.org/software/S0040>), ZXProxy, and ZXPortMap. (Citation: Trend Micro APT Attack Tools) Adversaries use these types of proxies to manage command and control communications, reduce the number of simultaneous outbound network connections, provide resiliency in the face of connection loss, or to ride over existing trusted communications paths between victims to

avoid suspicion. Adversaries may chain together multiple proxies to further disguise the source of malicious traffic. Adversaries can also take advantage of routing schemes in Content Delivery Networks (CDNs) to proxy command and control traffic.

Name

Ingress Tool Transfer

ID

T1105

Description

Adversaries may transfer tools or other files from an external system into a compromised environment. Tools or files may be copied from an external adversary-controlled system to the victim network through the command and control channel or through alternate protocols such as [ftp](https://attack.mitre.org/software/S0095). Once present, adversaries may also transfer/spread tools between victim devices within a compromised environment (i.e. [Lateral Tool Transfer](https://attack.mitre.org/techniques/T1570)). On Windows, adversaries may use various utilities to download tools, such as `copy`, `finger`, [certutil](https://attack.mitre.org/software/S0160), and [PowerShell](https://attack.mitre.org/techniques/T1059/001) commands such as `EX(New-Object Net.WebClient).downloadString()` and `Invoke-WebRequest`. On Linux and macOS systems, a variety of utilities also exist, such as `curl`, `scp`, `sftp`, `tftp`, `rsync`, `finger`, and `wget`. (Citation: t1105_lolbas) Adversaries may also abuse installers and package managers, such as `yum` or `winget`, to download tools to victim hosts. Files can also be transferred using various [Web Service](https://attack.mitre.org/techniques/T1102)s as well as native or otherwise present tools on the victim system.(Citation: PTSecurity Cobalt Dec 2016) In some cases, adversaries may be able to leverage services that sync between a web-based and an on-premises client, such as Dropbox or OneDrive, to transfer files onto victim systems. For example, by compromising a cloud account and logging into the service's web portal, an adversary may be able to trigger an automatic syncing process that transfers the file onto the victim's machine.(Citation: Dropbox Malware Sync)

Name

User Execution

ID

T1204

Description

An adversary may rely upon specific actions by a user in order to gain execution. Users may be subjected to social engineering to get them to execute malicious code by, for example, opening a malicious document file or link. These user actions will typically be observed as follow-on behavior from forms of [Phishing](https://attack.mitre.org/techniques/T1566). While [User Execution](https://attack.mitre.org/techniques/T1204) frequently occurs shortly after Initial Access it may occur at other phases of an intrusion, such as when an adversary places a file in a shared directory or on a user's desktop hoping that a user will click on it. This activity may also be seen shortly after [Internal Spearphishing](https://attack.mitre.org/techniques/T1534). Adversaries may also deceive users into performing actions such as enabling [Remote Access Software](https://attack.mitre.org/techniques/T1219), allowing direct control of the system to the adversary, or downloading and executing malware for [User Execution](https://attack.mitre.org/techniques/T1204). For example, tech support scams can be facilitated through [Phishing](https://attack.mitre.org/techniques/T1566), vishing, or various forms of user interaction. Adversaries can use a combination of these methods, such as spoofing and promoting toll-free numbers or call centers that are used to direct victims to malicious websites, to deliver and execute payloads containing malware or [Remote Access Software](https://attack.mitre.org/techniques/T1219). (Citation: Telephone Attack Delivery)

Name

T1071

ID

T1071

Description

Adversaries may communicate using OSI application layer protocols to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server. Adversaries may utilize many different protocols, including

those used for web browsing, transferring files, electronic mail, or DNS. For connections that occur internally within an enclave (such as those between a proxy or pivot node and other nodes), commonly used protocols are SMB, SSH, or RDP.

Sector

Name

Telecommunications

Description

Private and public entities involved in the production, transport and dissemination of information and communication signals.

StixFile

Value

827f41fc1a6f8a4c8a8575b3e2349aeaba0dfc2c9390ef1cceeef1bb85c34161

5cbafa2d562be0f5fa690f8d551cdb0bee9fc299959b749b99d44ae3fda782e4

External References

-
- <https://doubleagent.net/telecommunications/backdoor/gtp/2024/02/27/GTPDOOR-COVERT-TELCO-BACKDOOR>
-
- <https://otx.alienvault.com/pulse/65e63e81783f1d41b007f3ed>