Disrupting the GRIDTIDE Global Cyber Espionage Campaign

By Google Threat Intelligence Group, Mandiant

Published: 2026-02-25 · Archived: 2026-04-05 13:59:07 UTC

Introduction

Last week, Google Threat Intelligence Group (GTIG), Mandiant, and partners took action to disrupt a global espionage campaign targeting telecommunications and government organizations in dozens of nations across four continents. The threat actor, UNC2814, is a suspected People's Republic of China (PRC)-nexus cyber espionage group that GTIG has tracked since 2017. This prolific, elusive actor has a long history of targeting international governments and global telecommunications organizations across Africa, Asia, and the Americas and had confirmed intrusions in 42 countries when the disruption was executed. The attacker was using API calls to communicate with SaaS apps as command-and-control (C2) infrastructure to disguise their malicious traffic as benign, a common tactic used by threat actors when attempting to improve the stealth of their intrusions. Rather than abusing a weakness or security flaw, attackers rely on cloud-hosted products to function correctly and make their malicious traffic seem legitimate. This disruption, led by GTIG in partnership with other teams, included the following actions:

- Terminating all Google Cloud Projects controlled by the attacker, effectively severing their persistent access to environments compromised by the novel GRIDTIDE backdoor.
- Identifying and disabling all known UNC2814 infrastructure.
- Disabling attacker accounts and revoked access to the Google Sheets API calls leveraged by the actor for command-and-control (C2) purposes.
- Releasing a set of IOCs linked to UNC2814 infrastructure active since at least 2023.

GTIG’s understanding of this campaign was accelerated by a recent Mandiant Threat Defense investigation into UNC2814 activity. Mandiant discovered that UNC2814 was leveraging a novel backdoor tracked as GRIDTIDE. This activity is not the result of a security vulnerability in Google’s products; rather, it abuses legitimate Google Sheets API functionality to disguise C2 traffic.

As of Feb. 18, GTIG's investigation confirmed that UNC2814 has impacted 53 victims in 42 countries across four continents, and identified suspected infections in at least 20 more countries. It is important to highlight that UNC2814 has no observed overlaps with activity publicly reported as “Salt Typhoon,” and targets different victims globally using distinct tactics, techniques, and procedures (TTPs). Although the specific initial access vector for this campaign has not been determined, UNC2814 has a history of gaining entry by exploiting and compromising web servers and edge systems.

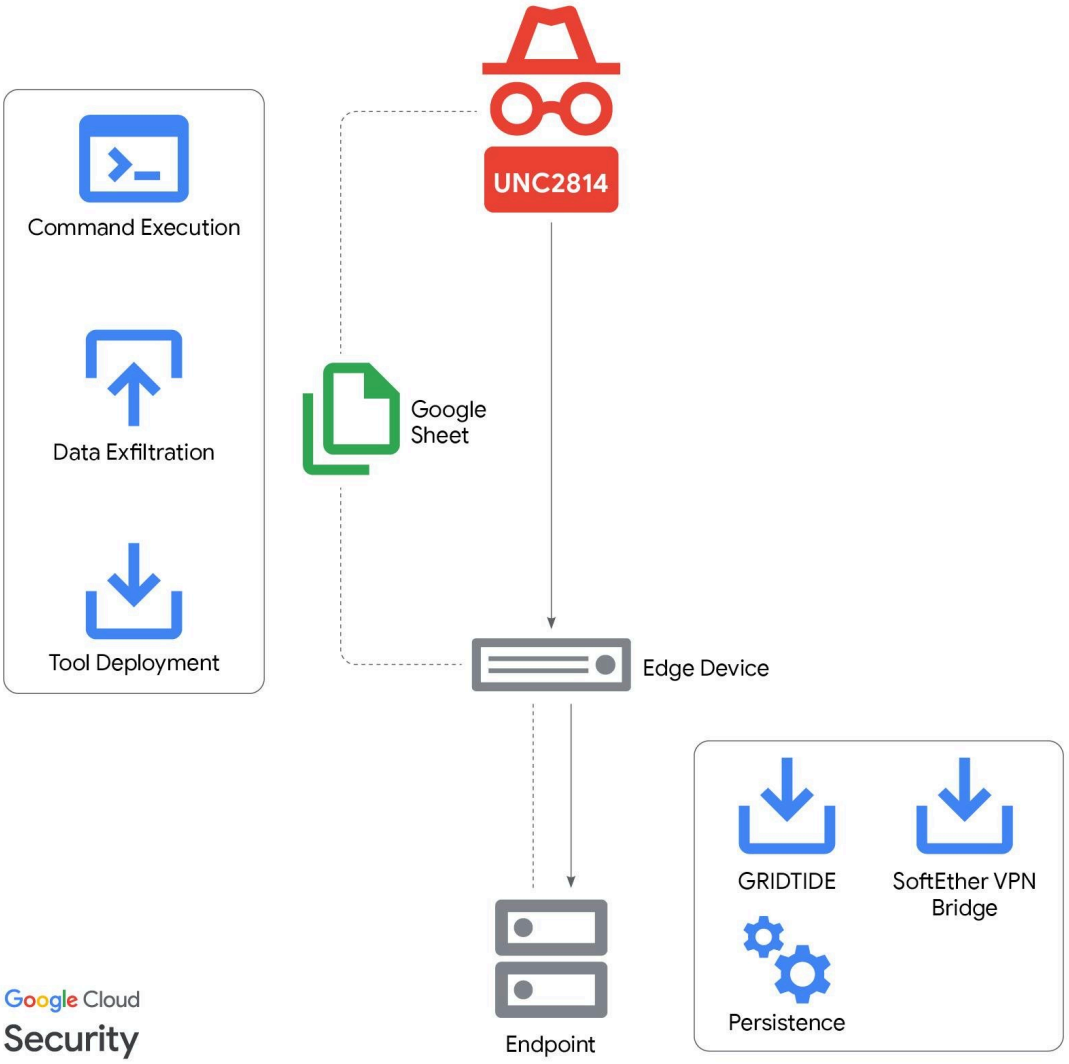

Figure 1:GRIDTIDE infection lifecycle

Initial Detection

Mandiant leverages Google Security Operations (SecOps) to perform continuous detection, investigation, and response across our global customer base. During this investigation, a detection flagged suspicious activity on a CentOS server.

In this case, Mandiant's investigation revealed a suspicious process tree: the binary `/var/tmp/xapt` initiated a shell with root privileges. The binary then executed the command `sh -c id 2>&1` to retrieve the system's user and group identifiers. This reconnaissance technique enabled the threat actor to confirm their successful privilege escalation to root. Mandiant analysts triaged the alert, confirmed the malicious intent, and reported the activity to the customer. This rapid identification of a sophisticated threat actor's TTPs demonstrates the value of Google Cloud's Shared Fate model, which provides organizations with curated, out-of-the-box (OOB) detection content designed to help organizations better defend against modern intrusions.

```
 [Process Tree]
/var/tmp/xapt
  └──── /bin/sh
```

```
        └──── sh -c id 2>&1
            └──── [Output] uid=0(root) gid=0(root) groups=0(root)
```

The payload was likely named `xapt` to masquerade as the legacy tool used in Debian-based systems.

Post-Compromise Activity

The threat actor used a service account to move laterally within the environment via SSH. Leveraging living-off-the-land (LotL)binaries, the threat actor performed reconnaissance activities, escalated privileges, and set up persistence for the GRIDTIDE backdoor.

To achieve persistence, the threat actor created a service for the malware at `/etc/systemd/system/xapt.service`, and once enabled, a new instance of the malware was spawned from `/usr/sbin/xapt`.

The threat actor initially executed GRIDTIDE via the command `nohup ./xapt`. This allows the backdoor to continue running even after the session is closed.

Subsequently, SoftEther VPN Bridge was deployed to establish an outbound encrypted connection to an external IP address. VPN configuration metadata suggests UNC2814 has been leveraging this specific infrastructure since July 2018.

The threat actor dropped GRIDTIDE on to an endpoint containing personally identifiable information (PII), including:

- Full name
- Phone number
- Date of birth
- Place of birth
- Voter ID number
- National ID number

We assess the targeting of PII in this engagement is consistent with cyber espionage activity in telecommunications, which is primarily leveraged to identify, track, and monitor persons of interest. We expect UNC2814 used this access to exfiltrate a variety of data on persons and their communications. Similar campaigns have been used to exfiltrate call data records, monitor SMS messages, and to even monitor targeted individuals through the telco’s lawful intercept capabilities.

GTIG did not directly observe UNC2814 exfiltrate sensitive data during this campaign. However, historical PRC-nexus espionage intrusions against telecoms have resulted in the theft of call data records, unencrypted SMS messages, and the compromise and abuse of lawful intercept systems. This focus on sensitive communications historically is intended to enable the targeting of individuals and organizations for surveillance efforts, particularly dissidents and activists, as well as traditional espionage targets. The access UNC2814 achieved during this campaign would likely enable clandestine efforts to similarly surveil targets.

GRIDTIDE

GRIDTIDE is a sophisticated C-based backdoor with the ability to execute arbitrary shell commands, upload files, and download files. The backdoor leverages Google Sheets as a high-availability C2 platform, treating the spreadsheet not as a document, but as a communication channel to facilitate the transfer of raw data and shell commands. GRIDTIDE hides its malicious traffic within legitimate cloud API requests, evading standard network detection. While the GRIDTIDE sample

FLARE analyzed as part of this campaign leverages Google Sheets for its C2, the actor could easily make use of other cloud-based spreadsheet platforms in the same manner.

Google Sheets

GRIDTIDE expects a 16-byte cryptographic key to be present in a separate file on the host at the time of execution. The malware uses this key to decrypt its Google Drive configurations using AES-128 in Cipher Block Chaining (CBC) mode.

The Google Drive configuration data contains the service account associated with UNC2814's Google Sheets document, and a private key for the account. It also contains the Google Spreadsheet ID and the private key to access the document. GRIDTIDE then connects to the malicious Google Spreadsheet using the Google Service Account for API authentication (the threat actor's Google Service Account and associated Google Workspace have been disabled).

When executed, GRIDTIDE sanitizes its Google Sheet. It does this by deleting the first 1000 rows, across columns A to Z in the spreadsheet, by using the Google Sheets API `batchClear` method. This prevents previous commands or file data stored in the Sheet from interfering with the threat actor's current session.

Once the Sheet is prepared, the backdoor conducts host-based reconnaissance. It fingerprints the endpoint by collecting the victim's username, endpoint name, OS details, local IP address, and environmental data such as the current working directory, language settings, and local time zone. This information is then exfiltrated and stored in cell V1 of the attacker-controlled spreadsheet.

Command Syntax

The threat actor issues instructions using a four-part command syntax: `<type>-<command_id>-<arg_1>-<arg_2>`.

- `<type>` Commands originating from the threat actor are categorized as type C (Client).
- `<command_id>`
  - `C` (Command): Executes Base64-encoded Bash shell commands on the endpoint and redirects the output to the spreadsheet.
  - `U` (Upload): Upload the data stored in the cells `A2:A<arg_2>` to the target endpoint, reconstruct and write to the encoded file path `<arg_1>`.
  - `D` (Download): Reads the data from the encoded local file path on the endpoint `<arg_1>` and transfers the contents in 45-KB fragments to the spreadsheet across the `A2:An` range.

In response, the malware posts a Server (`S`) status message to cell `A1`, confirming the successful completion of the task (`R`) or returning an error:

- `<type>` Responses originating from the malware are categorised as type `S` (Server).
- `<command_id>` Will match the `<command_id>` value sent by the threat actor.
- `<arg_1>` Indicating the command executed successfully (`R`), or an error message.
- `<arg_2>` Exfiltrated data is saved within the range `A2:A<arg_2>`. This value displays the upper cell number of the data.

Cell-Based C2

GRIDTIDE's C2 communication works on a cell-based polling mechanism, assigning specific roles to spreadsheet cells to facilitate communication.

- `A1` : The malware polls this cell via the Google Sheets API for attacker commands, and subsequently overwrites it with a status response upon completion (e.g., `S-C-R` or Server-Command-Success. If no command exists in the cell, the malware sleeps for one second before trying again. If the number of trials reaches 120, it changes the sleep time to be a random duration between 5–10 minutes, likely to reduce noise when the threat actor is not active. When a command does exist in the cell, GRIDTIDE executes it and resets the wait time to one second.
- `A2-An` : Used for the transfer of data, such as command output, uploading tools, or exfiltrating files.
- `V1` : Stores system data from the victim endpoint. When executed, the malware updates this cell with an encoded string containing host-based metadata.

Obfuscation and Evasion

To evade detection and web filtering, GRIDTIDE employs a URL-safe Base64 encoding scheme for all data sent and received. This encoding variant replaces standard Base64 characters (`+` and `/`) with alternatives (`-` and `_`).

Command Execution Lifecycle

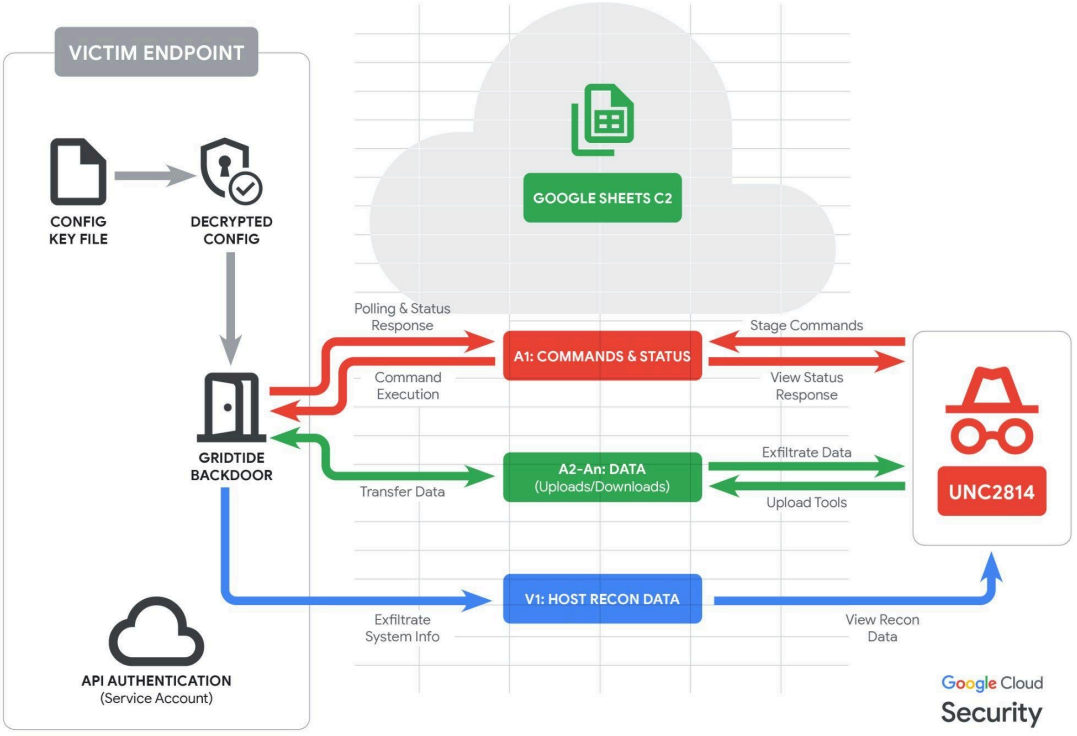

Figure 2: GRIDTIDE execution lifecycle

Targeting

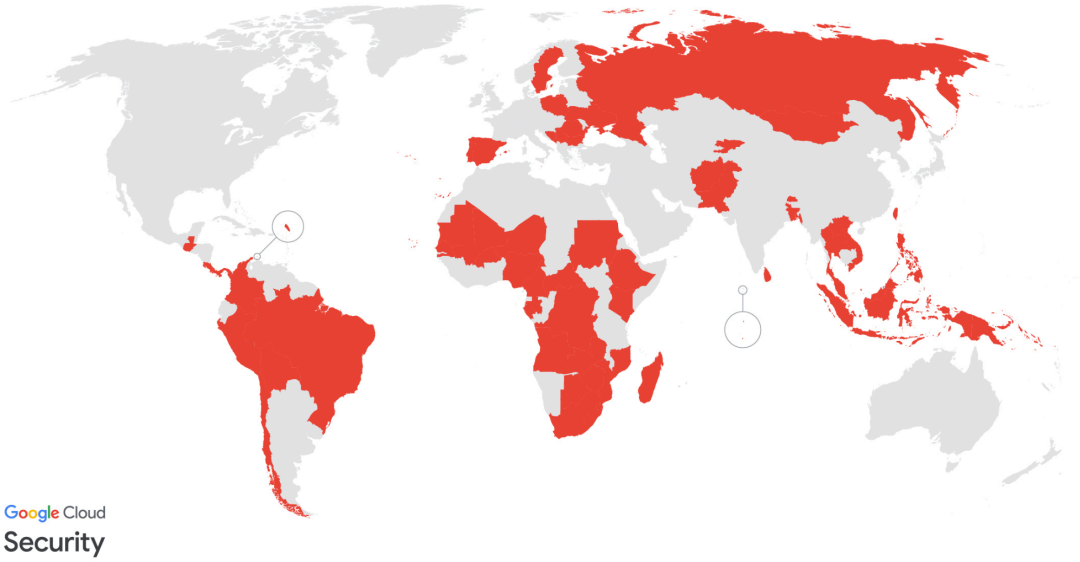

Figure 3: Countries with suspected or confirmed UNC2814 victims

UNC2814 is a suspected PRC-nexus threat actor that has conducted global operations since at least 2017. The group's recent activity leveraging GRIDTIDE malware has primarily focused on targeting telecommunications providers on a worldwide scale, but UNC2814 also targeted government organizations during this campaign.

GTIG confirmed 53 intrusions by UNC2814 in 42 total nations globally, and identified suspected targeting in at least 20 other nations. This prolific scope is likely the result of a decade of concentrated effort.

Disrupting UNC2814

GTIG is committed to actively countering and disrupting malicious operations, ensuring the safety of our customers and mitigating the global impact of this malicious cyber activity.

To counter UNC2814’s operations, GTIG executed a series of coordinated disruption actions:

- Elimination of GRIDTIDE Access: We terminated all Cloud Projects controlled by the attacker, effectively severing their persistent access to environments compromised by the GRIDTIDE backdoor.
- Infrastructure Takedown: In collaboration with partners, we identified and disabled all known UNC2814 infrastructure. This included the sinkholing of both current and historical domains used by the group in order to further dismantle UNC2814’s access to compromised environments.
- Account Disruption: GTIG and its partners disabled attacker accounts, revoked access to the Google Sheets, and disabled all Google Cloud projects leveraged by the actor for command-and-control (C2) purposes.
- Victim Notifications: GTIG has issued formal victim notifications and is actively supporting organizations with verified compromises resulting from this threat.
- Detection Signatures: We have refined and implemented a variety of signatures and signals designed to neutralize UNC2814 operations and intercept malware linked to GRIDTIDE.

- IOC Release: We are publicly releasing a collection of IOC's related to UNC2814 infrastructure that the group has used since at least 2023 to help organizations identify this activity in their networks and better protect customers and organizations around the world.

Conclusion

The global scope of UNC2814's activity, evidenced by confirmed or suspected operations in over 70 countries, underscores the serious threat facing telecommunications and government sectors, and the capacity for these intrusions to evade detection by defenders. Prolific intrusions of this scale are generally the result of years of focused effort and will not be easily re-established. We expect that UNC2814 will work hard to re-establish their global footprint.

Detection Through Google Security Operations

Google SecOps customers have access to these broad category rules and more under the Mandiant Hunting rule pack. The activity discussed in the blog post is detected in Google SecOps under the rule names:

- Suspicious Shell Execution From Var Directory
- Suspicious Sensitive File Access Via SSH
- Config File Staging in Sensitive Directories
- Shell Spawning Curl Archive Downloads from IP
- Numeric Permission Profiling in System Paths
- Sudo Shell Spawning Reconnaissance Tools
- Potential Google Sheets API Data Exfiltration

SecOps Hunting Queries

The following UDM queries can be used to identify potential compromises within your environment.

Suspicious Google Sheets API Connections

Search for a non-browser process initiating outbound HTTPS requests to specific Google Sheets URIs leveraged by GRIDTIDE.

```
 target.url = /sheets\.googleapis\.com/
(
  target.url = /batchClear/ OR
  target.url = /batchUpdate/ OR
  target.url = /valueRenderOption=FORMULA/
)
principal.process.file.full_path != /chrome|firefox|safari|msedge/
```

Config File Creation in Suspicious Directory

Identify configuration files being created at, modified, or moved to unexpected locations.

```
 (
  metadata.event_type = "FILE_CREATION" OR
  metadata.event_type = "FILE_MODIFICATION" OR
  metadata.event_type = "FILE_MOVE"
)
AND target.file.full_path = /^(\/usr\/sbin|\/sbin|\/var\/tmp)\/[^\\\/]+\.cfg$/ nocase
```

Suspicious Shell Execution from /var/tmp/

Detects executables with short alphanumeric filenames, launching from the /var/tmp/ directory, and spawning a shell.

```
 principal.process.file.full_path = /^\/var\/tmp\/[a-z0-9]{1,10}$/ nocase AND
target.process.file.full_path = /\b(ba)?sh$/ nocase
```

Indicators of Compromise (IOCs)

The following IOCs are available in a free Google Threat Intelligence (GTI) collection for registered users.

Host-Based Artifacts

Artifact	Description	Hash (SHA256)
xapt	GRIDTIDE	`ce36a5fc44cbd7de947130b67be9e732a7b4086fb1df98a5afd724087c973b47`
xapt.cfg	Key file used by GRIDTIDE to decrypt its Google Drive configuration.	`01fc3bd5a78cd59255a867ffb3dfdd6e0b7713ee90098ea96cc01c640c6495eb`
xapt.service	Malicious `systemd` service file created for GRIDTIDE persistence.	`eb08c840f4c95e2fa5eff05e5f922f86c766f5368a63476f046b2b9dbffc2033`
hamcore.se2	SoftEtherVPN Bridge component.	`4eb994b816a1a24cf97bfd7551d00fe14b810859170dbf15180d39e05cd7c0f9`
fire	SoftEtherVPN Bridge component (renamed from `vmlog`). Extracted	`4eb994b816a1a24cf97bfd7551d00fe14b810859170dbf15180d39e05cd7c0f9`

	from `update.tar.gz`.	
vpn_bridge.config	SoftEtherVPN Bridge configuration.	`669917bad46a57e5f2de037f8ec200a44fb579d723af3e2f1be1e8479a267966`
apt.tar.gz	Archive downloaded from `130.94.6[.]228`. Contained GRIDTIDE.	N/A
update.tar.gz	Additional archive downloaded. Contained `vmlog` (renamed to `fire`), a SoftEtherVPN Bridge component.	N/A
amp.tar.gz	Additional archive downloaded. Contained `hamcore.se2`, a SoftEtherVPN Bridge component.	N/A
pmp	GRIDTIDE variant.	N/A
pmp.cfg	GRIDTIDE variant key file.	N/A

Network-Based Artifacts

Type	Description	Artifact
IP	C2 server hosting `apt.tar.gz`,	`130[.]94[.]6[.]228`

	`update.tar.g` z, and `amp.tar.gz` .	
IP	Target of a `curl -ik` command to verify HTTPS access to their infrastructure.	`38[.]180[.]205[.]14`
IP	Threat actor's SoftEtherVPN server.	`38[.]60[.]194[.]21`
IP	Attacker IP	`38[.]54[.]112[.]184`
IP	Attacker IP	`38[.]60[.]171[.]242`
IP	Attacker IP	`195[.]123[.]211[.]70`
IP	Attacker IP	`202[.]59[.]10[.]122`
IP	Hosting malicious C2 domain.	`38[.]60[.]252[.]66`
IP	Hosting malicious C2 domain.	`45[.]76[.]184[.]214`
IP	Hosting malicious C2 domain.	`45[.]90[.]59[.]129`
IP	Hosting malicious C2 domain.	`195[.]123[.]226[.]235`
IP	Hosting malicious C2 domain.	`65[.]20[.]104[.]91`

IP	Hosting malicious C2 domain.	`5[.]34[.]176[.]6`
IP	Hosting malicious C2 domain.	`139[.]84[.]236[.]237`
IP	Hosting malicious C2 domain.	`149[.]28[.]128[.]128`
IP	Hosting malicious C2 domain.	`38[.]54[.]31[.]146`
IP	Hosting malicious C2 domain.	`178[.]79[.]188[.]181`
IP	Hosting malicious C2 domain.	`38[.]54[.]37[.]196`
IP	SoftEtherVPN server.	`207[.]148[.]73[.]18`
IP	SoftEtherVPN server.	`38[.]60[.]224[.]25`
IP	SoftEtherVPN server.	`149[.]28[.]139[.]125`
IP	SoftEtherVPN server.	`38[.]54[.]32[.]244`
IP	SoftEtherVPN server.	`38[.]54[.]82[.]69`
IP	SoftEtherVPN server.	`45[.]76[.]157[.]113`
IP	SoftEtherVPN server.	`45[.]77[.]254[.]168`
IP	SoftEtherVPN server.	`139[.]180[.]219[.]115`

User-Agent	GRIDTIDE User-Agent string.	`Directory API Google-API-Java-Client/2.0.0 Google-HTTP-Java-Client/1.42.3 (gzip)`
User-Agent	GRIDTIDE User-Agent string.	`Google-HTTP-Java-Client/1.42.3 (gzip)`
Domain	C2 domain	`1cv2f3d5s6a9w[.]ddnsfree[.]com`
Domain	C2 domain	`admina[.]freeddns[.]org`
Domain	C2 domain	`afsaces[.]accesscam[.]org`
Domain	C2 domain	`ancisesic[.]accesscam[.]org`
Domain	C2 domain	`applebox[.]camdvr[.]org`
Domain	C2 domain	`appler[.]kozow[.]com`
Domain	C2 domain	`asdad21ww[.]freeddns[.]org`
Domain	C2 domain	`aw2o25forsbc[.]camdvr[.]org`
Domain	C2 domain	`awcc001jdaigfwdagdcew[.]giize[.]com`
Domain	C2 domain	`bab2o25com[.]accesscam[.]org`
Domain	C2 domain	`babaji[.]accesscam[.]org`
Domain	C2 domain	`babi5599ss[.]ddnsgeek[.]com`
Domain	C2 domain	`balabalabo[.]mywire[.]org`

Domain	C2 domain	`bggs[.]giize[.]com`
Domain	C2 domain	`bibabo[.]freeddns[.]org`
Domain	C2 domain	`binmol[.]webredirect[.]org`
Domain	C2 domain	`bioth[.]giize[.]com`
Domain	C2 domain	`Boemobww[.]ddnsfree[.]com`
Domain	C2 domain	`brcallletme[.]theworkpc[.]com`
Domain	C2 domain	`btbtutil[.]theworkpc[.]com`
Domain	C2 domain	`btltan[.]ooguy[.]com`
Domain	C2 domain	`camcampkes[.]ddnsfree[.]com`
Domain	C2 domain	`camsqewivo[.]kozow[.]com`
Domain	C2 domain	`ccammutom[.]ddnsgeek[.]com`
Domain	C2 domain	`cdnvmtools[.]theworkpc[.]com`
Domain	C2 domain	`cloacpae[.]ddnsfree[.]com`
Domain	C2 domain	`cmwwoods1[.]theworkpc[.]com`
Domain	C2 domain	`cnrpaslceas[.]freeddns[.]org`
Domain	C2 domain	`codemicros12[.]gleeze[.]com`

Domain	C2 domain	`cressmiss[.]ooguy[.]com`
Domain	C2 domain	`cvabiasbae[.]ddnsfree[.]com`
Domain	C2 domain	`cvnoc01da1cjmnftsd[.]accesscam[.]org`
Domain	C2 domain	`cvpc01aenusocirem[.]accesscam[.]org`
Domain	C2 domain	`cvpc01cgsdfn53hgd[.]giize[.]com`
Domain	C2 domain	`DCLCWPDTSDCC[.]ddnsfree[.]com`
Domain	C2 domain	`dlpossie[.]ddnsfree[.]com`
Domain	C2 domain	`dnsfreedb[.]ddnsfree[.]com`
Domain	C2 domain	`doboudix1024[.]mywire[.]org`
Domain	C2 domain	`evilginx2[.]loseyourip[.]com`
Domain	C2 domain	`examp1e[.]webredirect[.]org`
Domain	C2 domain	`faeelt[.]giize[.]com`
Domain	C2 domain	`fakjcsaeyhs[.]ddnsfree[.]com`
Domain	C2 domain	`fasceadvcva3[.]gleeze[.]com`
Domain	C2 domain	`ffosies2024[.]camdvr[.]org`
Domain	C2 domain	`fgdedd1dww[.]gleeze[.]com`

Domain	C2 domain	`filipinet[.]ddnsgeek[.]com`
Domain	C2 domain	`freeios[.]theworkpc[.]com`
Domain	C2 domain	`ftpuser14[.]gleeze[.]com`
Domain	C2 domain	`ftpzpak[.]kozow[.]com`
Domain	C2 domain	`globoss[.]kozow[.]com`
Domain	C2 domain	`gogo2025up[.]ddnsfree[.]com`
Domain	C2 domain	`googlel[.]gleeze[.]com`
Domain	C2 domain	`googles[.]accesscam[.]org`
Domain	C2 domain	`googles[.]ddnsfree[.]com`
Domain	C2 domain	`googlett[.]camdvr[.]org`
Domain	C2 domain	`googllabwws[.]gleeze[.]com`
Domain	C2 domain	`gtaldps31c[.]ddnsfree[.]com`
Domain	C2 domain	`hamkorg[.]kozow[.]com`
Domain	C2 domain	`honidoo[.]loseyourip[.]com`
Domain	C2 domain	`huygdr12[.]loseyourip[.]com`
Domain	C2 domain	`icekancusjhea[.]ddnsgeek[.]com`

Domain	C2 domain	`idstandsuui[.]kozow[.]com`
Domain	C2 domain	`indoodchat[.]theworkpc[.]com`
Domain	C2 domain	`jarvis001[.]freeddns[.]org`
Domain	C2 domain	`Kaushalya[.]freeddns[.]org`
Domain	C2 domain	`khyes001ndfpnuewdm[.]kozow[.]com`
Domain	C2 domain	`kskxoscieontrolanel[.]gleeze[.]com`
Domain	C2 domain	`ksv01sokudwongsj[.]theworkpc[.]com`
Domain	C2 domain	`lcskiecjj[.]loseyourip[.]com`
Domain	C2 domain	`lcskiecs[.]ddnsfree[.]com`
Domain	C2 domain	`losiesca[.]ddnsgeek[.]com`
Domain	C2 domain	`lps2staging[.]ddnsfree[.]com`
Domain	C2 domain	`lsls[.]casacam[.]net`
Domain	C2 domain	`ltiuys[.]ddnsgeek[.]com`
Domain	C2 domain	`ltiuys[.]kozow[.]com`
Domain	C2 domain	`mailsdy[.]gleeze[.]com`
Domain	C2 domain	`maliclick1[.]ddnsfree[.]com`

Domain	C2 domain	`mauritasszddb[.]ddnsfree[.]com`
Domain	C2 domain	`meetls[.]kozow[.]com`
Domain	C2 domain	`Microsoft[.]bumbleshrimp[.]com`
Domain	C2 domain	`ml3[.]freeddns[.]org`
Domain	C2 domain	`mlksucnayesk[.]kozow[.]com`
Domain	C2 domain	`mmmfaco2025[.]mywire[.]org`
Domain	C2 domain	`mms[.]bumbleshrimp[.]com`
Domain	C2 domain	`mmvmtools[.]giize[.]com`
Domain	C2 domain	`modgood[.]gleeze[.]com`
Domain	C2 domain	`Mosplosaq[.]accesscam[.]org`
Domain	C2 domain	`mysql[.]casacam[.]net`
Domain	C2 domain	`nenigncagvawr[.]giize[.]com`
Domain	C2 domain	`nenignenigoncqvoo[.]ooguy[.]com`
Domain	C2 domain	`nenigoncqnutgo[.]accesscam[.]org`
Domain	C2 domain	`nenigoncuopzc[.]giize[.]com`
Domain	C2 domain	`nims[.]gleeze[.]com`

Domain	C2 domain	`nisaldwoa[.]theworkpc[.]com`
Domain	C2 domain	`nmszablogs[.]ddnsfree[.]com`
Domain	C2 domain	`nodekeny11[.]freeddns[.]org`
Domain	C2 domain	`nodjs2o25nodjs[.]giize[.]com`
Domain	C2 domain	`Npeoples[.]theworkpc[.]com`
Domain	C2 domain	`officeshan[.]kozow[.]com`
Domain	C2 domain	`okkstt[.]ddnsgeek[.]com`
Domain	C2 domain	`oldatain1[.]ddnsgeek[.]com`
Domain	C2 domain	`onlyosun[.]ooguy[.]com`
Domain	C2 domain	`osix[.]ddnsgeek[.]com`
Domain	C2 domain	`ovmmiuy[.]mywire[.]org`
Domain	C2 domain	`palamolscueajfvc[.]gleeze[.]com`
Domain	C2 domain	`pawanp[.]kozow[.]com`
Domain	C2 domain	`pcmainecia[.]ddnsfree[.]com`
Domain	C2 domain	`pcvmts3[.]kozow[.]com`
Domain	C2 domain	`peisuesacae[.]loseyourip[.]com`

Domain	C2 domain	`peowork[.]ddnsgeek[.]com`
Domain	C2 domain	`pepesetup[.]ddnsfree[.]com`
Domain	C2 domain	`pewsus[.]freeddns[.]org`
Domain	C2 domain	`plcoaweniva[.]ddnsgeek[.]com`
Domain	C2 domain	`PolicyAgent[.]theworkpc[.]com`
Domain	C2 domain	`polokinyea[.]gleeze[.]com`
Domain	C2 domain	`pplodsssead222[.]loseyourip[.]com`
Domain	C2 domain	`pplosad231[.]kozow[.]com`
Domain	C2 domain	`ppsaBedon[.]gleeze[.]com`
Domain	C2 domain	`prdanjana01[.]ddnsfree[.]com`
Domain	C2 domain	`prepaid127[.]freeddns[.]org`
Domain	C2 domain	`PRIFTP[.]kozow[.]com`
Domain	C2 domain	`prihxlcs[.]ddnsfree[.]com`
Domain	C2 domain	`prihxlcsw[.]theworkpc[.]com`
Domain	C2 domain	`pxlaxvvva[.]freeddns[.]org`
Domain	C2 domain	`quitgod2023luck[.]giize[.]com`

Domain	C2 domain	`rabbit[.]ooguy[.]com`
Domain	C2 domain	`rsm323[.]kozow[.]com`
Domain	C2 domain	`saf3asg[.]giize[.]com`
Domain	C2 domain	`Scopps[.]ddnsgeek[.]com`
Domain	C2 domain	`sdhite43[.]ddnsfree[.]com`
Domain	C2 domain	`sdsuytoins63[.]kozow[.]com`
Domain	C2 domain	`selfad[.]gleeze[.]com`
Domain	C2 domain	`serious[.]kozow[.]com`
Domain	C2 domain	`setupcodpr2[.]freeddns[.]org`
Domain	C2 domain	`sgsn[.]accesscam[.]org`
Domain	C2 domain	`Smartfren[.]giize[.]com`
Domain	C2 domain	`sn0son4t31bbsvopou[.]camdvr[.]org`
Domain	C2 domain	`sn0son4t31opc[.]freeddns[.]org`
Domain	C2 domain	`soovuy[.]gleeze[.]com`
Domain	C2 domain	`styuij[.]mywire[.]org`
Domain	C2 domain	`supceasfg1[.]loseyourip[.]com`

Domain	C2 domain	`systemsz[.]kozow[.]com`
Domain	C2 domain	`t31c0mjumpcuyerop[.]ooguy[.]com`
Domain	C2 domain	`t31c0mopamcuiomx[.]kozow[.]com`
Domain	C2 domain	`t31c0mopmiuewklg[.]webredirect[.]org`
Domain	C2 domain	`t31c0mopocuveop[.]accesscam[.]org`
Domain	C2 domain	`t3lc0mcanyqbfac[.]loseyourip[.]com`
Domain	C2 domain	`t3lc0mczmoihwc[.]camdvr[.]org`
Domain	C2 domain	`t3lc0mh4udncifw[.]casacam[.]net`
Domain	C2 domain	`t3lc0mhasvnctsk[.]giize[.]com`
Domain	C2 domain	`t3lm0rtlcagratu[.]kozow[.]com`
Domain	C2 domain	`tch[.]giize[.]com`
Domain	C2 domain	`telcomn[.]giize[.]com`
Domain	C2 domain	`telen[.]bumbleshrimp[.]com`
Domain	C2 domain	`telkom[.]ooguy[.]com`
Domain	C2 domain	`telkomservices[.]theworkpc[.]com`
Domain	C2 domain	`thbio[.]kozow[.]com`

Domain	C2 domain	`timpe[.]kozow[.]com`
Domain	C2 domain	`timpe[.]webredirect[.]org`
Domain	C2 domain	`tlse001hdfuwwgdgpnn[.]theworkpc[.]com`
Domain	C2 domain	`tltlsktelko[.]ddnsfree[.]com`
Domain	C2 domain	`transport[.]dynuddns[.]net`
Domain	C2 domain	`trvcl[.]bumbleshrimp[.]com`
Domain	C2 domain	`ttsiou12[.]loseyourip[.]com`
Domain	C2 domain	`ua2o25yth[.]ddnsgeek[.]com`
Domain	C2 domain	`udieyg[.]gleeze[.]com`
Domain	C2 domain	`unnjunnani[.]ddnsfree[.]com`
Domain	C2 domain	`updatamail[.]kozow[.]com`
Domain	C2 domain	`updatasuccess[.]ddnsgeek[.]com`
Domain	C2 domain	`updateservices[.]kozow[.]com`
Domain	C2 domain	`updatetools[.]giize[.]com`
Domain	C2 domain	`uscplxsecjs[.]ddnsgeek[.]com`
Domain	C2 domain	`USOShared1[.]ddnsfree[.]com`

Domain	C2 domain	`vals[.]bumbleshrimp[.]com`
Domain	C2 domain	`vass[.]ooguy[.]com`
Domain	C2 domain	`vass2025[.]casacam[.]net`
Domain	C2 domain	`vmtools[.]camdvr[.]org`
Domain	C2 domain	`vmtools[.]loseyourip[.]com`
Domain	C2 domain	`vosies[.]ddnsfree[.]com`
Domain	C2 domain	`vpaspmine[.]freeddns[.]org`
Domain	C2 domain	`wdlcamaakc[.]ooguy[.]com`
Domain	C2 domain	`winfoss1[.]kozow[.]com`
Domain	C2 domain	`ysiohbk[.]camdvr[.]org`
Domain	C2 domain	`zammffayhd[.]ddnsfree[.]com`
Domain	C2 domain	`zmcmvmbm[.]ddnsfree[.]com`
Domain	C2 domain	`zwmn350n3o1fsdf3gs[.]kozow[.]com`
Domain	C2 domain	`zwmn350n3o1ugety2xbe[.]camdvr[.]org`
Domain	C2 domain	`zwmn350n3o1vsdrggs[.]ddnsfree[.]com`
Domain	C2 domain	`zwt310n3o1unety2kab[.]webredirect[.]org`

Domain	C2 domain	`zwt310n3o2unety6a3k[.]kozow[.]com`
Domain	C2 domain	`zwt31n3t0nidoqmve[.]camdvr[.]org`
Domain	C2 domain	`zwt3ln3t1aimckalw[.]theworkpc[.]com`
SHA256 Hash	Self-signed X.509 SSL certificate	`d25024ccea8eac85a9522289cfb709f2ed4e20176dd37855bacc2cd75c995606`

Description	**URLs**
Archive contained GRIDTIDE.	`http://130[.]94[.]6[.]228/apt.tar.gz`
Archive contained a SoftEtherVPN Bridge component.	`http://130[.]94[.]6[.]228/update.tar.gz`
Archive contained a SoftEtherVPN Bridge component.	`http://130[.]94[.]6[.]228/amp.tar.gz`
GRIDTIDE leverages this API endpoint to monitor cell A1 of the spreadsheet for threat actor commands.	`https://sheets[.]googleapis[.]com:443/v4/spreadsheets/<GoogleSheetID>/values/A1?valueRenderOption=FORMULA`

GRIDTIDE leverages this API endpoint to clear data from the first 1000 rows of the spreadsheet.	`https://sheets[.]googleapis[.]com:443/v4/spreadsheets/<GoogleSheetID>/values:batchClear`
GRIDTIDE leverages this API endpoint to exfiltrate victim host metadata to cell `V1`, report command execution output and status messages to cell `A1`, and to transfer data into the `A2:An` cell range.	`https://sheets[.]googleapis[.]com:443/v4/spreadsheets/<GoogleSheetID>/values:batchUpdate`
GRIDTIDE leverages this API endpoint to transfer data from the `A2:An` cell range to the victim host.	`https://sheets[.]googleapis[.]com:443/v4/spreadsheets/<GoogleSheetID>/values/A2:A<cell_number>?valueRenderOption=FORMULA`

GRIDTIDE YARA Rule

```
rule G_APT_Backdoor_GRIDTIDE_1 {
        meta:
                author = "Google Threat Intelligence Group (GTIG)"
        strings:
```

```
                $s1 = { 7B 22 61 6C 67 22 3A 22 52 53 32 35 36 22 2C 22 6B 69 64 22 3A 22 25 73 22 2C 22 74 79 70 22 3A
                $s2 = { 2F 70 72 6F 63 2F 73 65 6C 66 2F 65 78 65 00 }
                $s3 = { 7B 22 72 61 6E 67 65 73 22 3A 5B 22 61 31 3A 7A 31 30 30 30 22 5D 7D 00 }
                $s4 = { 53 2D 55 2D 25 73 2D 31 00 }
                $s5 = { 53 2D 55 2D 52 2D 31 00 }
                $s6 = { 53 2D 44 2D 25 73 2D 30 00 }
                $s7 = { 53 2D 44 2D 52 2D 25 64 00 }
        condition:
                (uint32(0) == 0x464c457f) and 6 of ($*)
}
```

Posted in

- Threat Intelligence

Source: https://cloud.google.com/blog/topics/threat-intelligence/disrupting-gridtide-global-espionage-campaign/