ADVISORY FOR ICM SECTOR

UNC2814 “GRIDTIDE” Cyber-Espionage Campaign Against Global Telecoms

Original report published on: February 26, 2026[1]

Executive Summary

On 26 February 2026, Google Threat Intelligence Group (GTIG) reported a cyber-espionage campaign attributed to UNC2814, which targeted at least 53 organisations across 42 countries. The activity affected telecommunications operators and government entities in Africa, Asia, America, and other regions. The Theat Actor (TA) used a custom C-based backdoor, GRIDTIDE, that abuses legitimate Google Sheets API calls for command-and-control (C2) to run commands, move files, and fingerprint endpoints while blending into normal SaaS traffic. Initial access in this campaign remains under investigation. After compromising internet-facing web servers and edge systems, UNC2814 moves laterally via SSH using service accounts and living-off-the-land (LotL) binaries to systems containing subscriber personally identifiable information (PII), call records or SMS information. During this campaign, there was no observation of data exfiltration.

Background

UNC2814 has been active since 2017 and uses GRIDTIDE backdoor embedded with an encrypted configuration that holds Google service account credentials, spreadsheet IDs, and private keys. UNC2814 abuses Google Sheets – a free to use spreadsheet service. GRIDTIDE would batch-clear the first 1,000 rows (columns A–Z), so that it is ready to store reconnaissance results from targeted systems where username, hostname, operating system, IP address, locale, and timezone is collected. GRIDTIDE polls a specific Google Sheet cell (such as A1) via API for attacker commands, then uses predefined cells to handle tasking, status updates, and data exfiltration.

GRIDTIDE uses URL-safe Base64 encoding which disguises activity as normal API usage in SaaS environments. For command and control, UNC2814 deploys SoftEther VPN Bridge to create encrypted outbound tunnels and established a systemd service at */etc/systemd/system/xapt.service*. Once enabled, this service spawned a new malware instance from */usr/sbin/xapt* for persistence.

Google has since terminated this TA’s attacker-controlled Google Cloud projects, accounts and access to the Google Sheets API. UNC2814’s GRIDTIDE C2 infrastructure has been taken offline, including current and historical domains. Indicators of compromise (IOCs) and detection signatures have been published so that organisations can identify and block related activity.

Detection and Mitigation

IMDA recommends that organisations perform continual testing and validation of existing security controls to ensure detection and prevention of GRIDTIDE-related activities identified in this advisory:

- Scan for Indicators of Compromise (Annex A) to detect threat activities in your environment.

- Refer to the MITRE ATT&CK techniques (Annex B) in this advisory to:
  - Create, test and validate detection rules against the threat behaviours.
  - Validate and deny or disable processes, ports and protocols that have no legitimate business need.
- Prioritise patching internet facing web servers and edge appliances to the latest versions.
- Segment the network so a compromised web or edge host cannot freely initiate SSH across the environment and only allow SSH from pre-approved IP addresses.
- Enforce egress controls for SaaS APIs and enable TLS inspection where feasible to detect unusual Google Sheets API activity, especially high volume read/write operations originating from servers.
- Apply least privilege to service accounts, restrict which host can be accessed over SSH, and rotate SSH keys regularly to limit opportunities for lateral movement.
- Deploy the GRIDTIDE YARA rule (Annex C) on capable platforms such as Endpoint Detection and Response (EDR) to detect and correlate GRIDTIDE related activity.
- Create SIEM rules to detect abnormal use of living off the land binaries such as *sh*, *id* and *nohup* on high-value servers, focusing on executions from unusual directories or suspicious process chains that establish network connections.
- Deploy network detection and response (NDR) tool to monitor and alert staff on new or unusual encrypted outbound traffic from servers, particularly VPN-like tunnels (detected via TLS fingerprinting) and SoftEther-related services. Validate each instance and deny unauthorised traffic.
- Create detection rules against Linux system logs on SIEM where operators will monitor for unauthorised systemd service creation and for binaries executing from paths such as */var/tmp* and */usr/sbin*.

IMDA encourages organisations to conduct thorough analyses to identify potential risks and assess their potential impact prior to deploying defensive measures.

Annex A - Indicators of Compromise

Type	Value	Comment
IP	130[.]94[.]6[.]228	C2 server hosting apt.tar.gz, update.tar.gz, and amp.tar.gz.
IP	38[.]180[.]205[.]14	Target of a curl -ik command to verify HTTPS access to their infrastructure.
IP	38[.]60[.]194[.]21	Threat actor's SoftEtherVPN server.
IP	38[.]54[.]112[.]184	Attacker IP
IP	38[.]60[.]171[.]242	Attacker IP
IP	195[.]123[.]211[.]70	Attacker IP
IP	202[.]59[.]10[.]122	Attacker IP
IP	38[.]60[.]252[.]66	Hosting malicious C2 domain.
IP	45[.]76[.]184[.]214	Hosting malicious C2 domain.
IP	45[.]90[.]59[.]129	Hosting malicious C2 domain.
IP	195[.]123[.]226[.]235	Hosting malicious C2 domain.
IP	65[.]20[.]104[.]91	Hosting malicious C2 domain.
IP	5[.]34[.]176[.]6	Hosting malicious C2 domain.
IP	139[.]84[.]236[.]237	Hosting malicious C2 domain.
IP	149[.]28[.]128[.]128	Hosting malicious C2 domain.
IP	38[.]54[.]31[.]146	Hosting malicious C2 domain.
IP	178[.]79[.]188[.]181	Hosting malicious C2 domain.
IP	38[.]54[.]37[.]196	Hosting malicious C2 domain.
IP	207[.]148[.]73[.]18	SoftEtherVPN server.
IP	38[.]60[.]224[.]25	SoftEtherVPN server.
IP	149[.]28[.]139[.]125	SoftEtherVPN server.
IP	38[.]54[.]32[.]244	SoftEtherVPN server.
IP	38[.]54[.]82[.]69	SoftEtherVPN server.
IP	45[.]76[.]157[.]113	SoftEtherVPN server.
IP	45[.]77[.]254[.]168	SoftEtherVPN server.
IP	139[.]180[.]219[.]115	SoftEtherVPN server.
IP	103[.]232[.]123[.]254	-
IP	136[.]244[.]66[.]16	-
IP	139[.]180[.]189[.]85	-
IP	139[.]180[.]222[.]59	-
IP	172[.]232[.]236[.]160	-
IP	185[.]93[.]173[.]44	-
IP	38[.]60[.]171[.]123	-
domain	1cv2f3d5s6a9w[.]ddnsfree[.]com	C2 domain
domain	admina[.]freeddns[.]org	C2 domain
domain	afsaces[.]accesscam[.]org	C2 domain
domain	ancisesic[.]accesscam[.]org	C2 domain
domain	applebox[.]camdvr[.]org	C2 domain
domain	appler[.]kozow[.]com	C2 domain
domain	asdad21ww[.]freeddns[.]org	C2 domain

domain	aw2o25forsbc[.]camdvr[.]org	C2 domain
domain	awcc001jdaigfwdagdcew[.]giize[.]com	C2 domain
domain	bab2o25com[.]accesscam[.]org	C2 domain
domain	babaji[.]accesscam[.]org	C2 domain
domain	babi5599ss[.]ddnsgeek[.]com	C2 domain
domain	balabalabo[.]mywire[.]org	C2 domain
domain	bggs[.]giize[.]com	C2 domain
domain	bibabo[.]freeddns[.]org	C2 domain
domain	binmol[.]webredirect[.]org	C2 domain
domain	bioth[.]giize[.]com	C2 domain
domain	boemobww[.]ddnsfree[.]com	C2 domain
domain	brcallletme[.]theworkpc[.]com	C2 domain
domain	btbtutil[.]theworkpc[.]com	C2 domain
domain	btltan[.]ooguy[.]com	C2 domain
domain	camcampkes[.]ddnsfree[.]com	C2 domain
domain	camsqewivo[.]kozow[.]com	C2 domain
domain	ccammutom[.]ddnsgeek[.]com	C2 domain
domain	ccel[.]kozow[.]com	C2 domain
domain	cd4fr1c3l1cscz0bak[.]kozow[.]com	C2 domain
domain	cd4fr1c3l1hyagv1cd[.]ooguy[.]com	C2 domain
domain	cdnvmtools[.]theworkpc[.]com	C2 domain
domain	cloacpae[.]ddnsfree[.]com	C2 domain
domain	cmwwoods1[.]theworkpc[.]com	C2 domain
domain	cnrpaslceas[.]freeddns[.]org	C2 domain
domain	codemicros12[.]gleeze[.]com	C2 domain
domain	cressmiss[.]ooguy[.]com	C2 domain
domain	cvabiasbae[.]ddnsfree[.]com	C2 domain
domain	cvnoc01da1cjmnftsd[.]accesscam[.]org	C2 domain
domain	cvpc01aenusocirem[.]accesscam[.]org	C2 domain
domain	cvpc01cgsdfn53hgd[.]giize[.]com	C2 domain
domain	dclcwpdtsdcc[.]ddnsfree[.]com	C2 domain
domain	dlpossie[.]ddnsfree[.]com	C2 domain
domain	dnsfreedb[.]ddnsfree[.]com	C2 domain
domain	doboudix1024[.]mywire[.]org	C2 domain
domain	entel[.]kozow[.]com	C2 domain
domain	evilginx2[.]loseyourip[.]com	C2 domain
domain	faeelt[.]giize[.]com	C2 domain
domain	fakjcsaeyhs[.]ddnsfree[.]com	C2 domain
domain	fasceadvcva3[.]gleeze[.]com	C2 domain
domain	ffosies2024[.]camdvr[.]org	C2 domain
domain	fgdedd1dww[.]gleeze[.]com	C2 domain
domain	filipinet[.]ddnsgeek[.]com	C2 domain
domain	freeios[.]theworkpc[.]com	C2 domain

domain	ftpuser14[.]gleeze[.]com	C2 domain
domain	ftpzpak[.]kozow[.]com	C2 domain
domain	globoss[.]kozow[.]com	C2 domain
domain	googlel[.]gleeze[.]com	C2 domain
domain	googles[.]accesscam[.]org	C2 domain
domain	googles[.]ddnsfree[.]com	C2 domain
domain	googlett[.]camdvr[.]org	C2 domain
domain	googllabwws[.]gleeze[.]com	C2 domain
domain	gtaldps31c[.]ddnsfree[.]com	C2 domain
domain	hamkorg[.]kozow[.]com	C2 domain
domain	honidoo[.]loseyourip[.]com	C2 domain
domain	huygdr12[.]loseyourip[.]com	C2 domain
domain	icekancusjhea[.]ddnsgeek[.]com	C2 domain
domain	idstandsuui[.]kozow[.]com	C2 domain
domain	indoodchat[.]theworkpc[.]com	C2 domain
domain	jarvis001[.]freeddns[.]org	C2 domain
domain	kaushalya[.]freeddns[.]org	C2 domain
domain	khyes001ndfpnuewdm[.]kozow[.]com	C2 domain
domain	kskxoscieontrolanel[.]gleeze[.]com	C2 domain
domain	ksv01sokudwongsj[.]theworkpc[.]com	C2 domain
domain	lcskiecjj[.]loseyourip[.]com	C2 domain
domain	lcskiecs[.]ddnsfree[.]com	C2 domain
domain	losiesca[.]ddnsgeek[.]com	C2 domain
domain	lps2staging[.]ddnsfree[.]com	C2 domain
domain	lsls[.]casacam[.]net	C2 domain
domain	ltiuys[.]ddnsgeek[.]com	C2 domain
domain	ltiuys[.]kozow[.]com	C2 domain
domain	mailsdy[.]gleeze[.]com	C2 domain
domain	maliclick1[.]ddnsfree[.]com	C2 domain
domain	mauritasszddb[.]ddnsfree[.]com	C2 domain
domain	meetls[.]kozow[.]com	C2 domain
domain	microsoft[.]bumbleshrimp[.]com	C2 domain
domain	ml3[.]freeddns[.]org	C2 domain
domain	mlksucnayesk[.]kozow[.]com	C2 domain
domain	mmmfaco2025[.]mywire[.]org	C2 domain
domain	mms[.]bumbleshrimp[.]com	C2 domain
domain	mmvmtools[.]giize[.]com	C2 domain
domain	modgood[.]gleeze[.]com	C2 domain
domain	mosplosaq[.]accesscam[.]org	C2 domain
domain	mysql[.]casacam[.]net	C2 domain
domain	nenigncagvawr[.]giize[.]com	C2 domain
domain	nenignenigoncqvoo[.]ooguy[.]com	C2 domain
domain	nenigoncqnutgo[.]accesscam[.]org	C2 domain
domain	nenigoncuopzc[.]giize[.]com	C2 domain

domain	nims[.]gleeze[.]com	C2 domain
domain	nisaldwoa[.]theworkpc[.]com	C2 domain
domain	nmszablogs[.]ddnsfree[.]com	C2 domain
domain	nodekeny11[.]freeddns[.]org	C2 domain
domain	nodjs2o25nodjs[.]giize[.]com	C2 domain
domain	npeoples[.]theworkpc[.]com	C2 domain
domain	officeshan[.]kozow[.]com	C2 domain
domain	okkstt[.]ddnsgeek[.]com	C2 domain
domain	oldatain1[.]ddnsgeek[.]com	C2 domain
domain	onlyosun[.]ooguy[.]com	C2 domain
domain	osix[.]ddnsgeek[.]com	C2 domain
domain	ovmmiuy[.]mywire[.]org	C2 domain
domain	palamolscueajfvc[.]gleeze[.]com	C2 domain
domain	pawanp[.]kozow[.]com	C2 domain
domain	pcmainecia[.]ddnsfree[.]com	C2 domain
domain	pcvmts3[.]kozow[.]com	C2 domain
domain	peisuesacae[.]loseyourip[.]com	C2 domain
domain	peowork[.]ddnsgeek[.]com	C2 domain
domain	pepesetup[.]ddnsfree[.]com	C2 domain
domain	pewsus[.]freeddns[.]org	C2 domain
domain	plcoaweniva[.]ddnsgeek[.]com	C2 domain
domain	policyagent[.]theworkpc[.]com	C2 domain
domain	polokinyea[.]gleeze[.]com	C2 domain
domain	pplodsssead222[.]loseyourip[.]com	C2 domain
domain	pplosad231[.]kozow[.]com	C2 domain
domain	ppsabedon[.]gleeze[.]com	C2 domain
domain	prdanjana01[.]ddnsfree[.]com	C2 domain
domain	prepaid127[.]freeddns[.]org	C2 domain
domain	priftp[.]kozow[.]com	C2 domain
domain	prihxlcs[.]ddnsfree[.]com	C2 domain
domain	prihxlcsw[.]theworkpc[.]com	C2 domain
domain	pxlaxvvva[.]freeddns[.]org	C2 domain
domain	quitgod2023luck[.]giize[.]com	C2 domain
domain	rabbit[.]ooguy[.]com	C2 domain
domain	rsm323[.]kozow[.]com	C2 domain
domain	saf3asg[.]giize[.]com	C2 domain
domain	scopps[.]ddnsgeek[.]com	C2 domain
domain	sdhite43[.]ddnsfree[.]com	C2 domain
domain	sdsuytoins63[.]kozow[.]com	C2 domain
domain	selfad[.]gleeze[.]com	C2 domain
domain	serious[.]kozow[.]com	C2 domain
domain	setupcodpr2[.]freeddns[.]org	C2 domain
domain	sgsn[.]accesscam[.]org	C2 domain
domain	smartfren[.]giize[.]com	C2 domain
domain	sn0son4t31bbsvopou[.]camdvr[.]org	C2 domain
domain	sn0son4t31opc[.]freeddns[.]org	C2 domain

domain	soovuy[.]gleeze[.]com	C2 domain
domain	styuij[.]mywire[.]org	C2 domain
domain	supceasfg1[.]loseyourip[.]com	C2 domain
domain	systemsz[.]kozow[.]com	C2 domain
domain	t31c0mjumpcuyerop[.]ooguy[.]com	C2 domain
domain	t31c0mopamcuiomx[.]kozow[.]com	C2 domain
domain	t31c0mopmiuewklg[.]webredirect[.]org	C2 domain
domain	t31c0mopocuveop[.]accesscam[.]org	C2 domain
domain	t3lc0mcanyqbfac[.]loseyourip[.]com	C2 domain
domain	t3lc0mczmoihwc[.]camdvr[.]org	C2 domain
domain	t3lc0mh4udncifw[.]casacam[.]net	C2 domain
domain	t3lc0mhasvnctsk[.]giize[.]com	C2 domain
domain	t3lm0rtlcagratu[.]kozow[.]com	C2 domain
domain	tch[.]giize[.]com	C2 domain
domain	telcomn[.]giize[.]com	C2 domain
domain	telen[.]bumbleshrimp[.]com	C2 domain
domain	telkom[.]ooguy[.]com	C2 domain
domain	telkomservices[.]theworkpc[.]com	C2 domain
domain	thbio[.]kozow[.]com	C2 domain
domain	timpe[.]kozow[.]com	C2 domain
domain	timpe[.]webredirect[.]org	C2 domain
domain	tlse001hdfuwwgdgpnn[.]theworkpc[.]com	C2 domain
domain	tltlsktelko[.]ddnsfree[.]com	C2 domain
domain	togo[.]giize[.]com	C2 domain
domain	transport[.]dynuddns[.]net	C2 domain
domain	trvcl[.]bumbleshrimp[.]com	C2 domain
domain	ttsiou12[.]loseyourip[.]com	C2 domain
domain	ua2o25yth[.]ddnsgeek[.]com	C2 domain
domain	udieyg[.]gleeze[.]com	C2 domain
domain	unnjunnani[.]ddnsfree[.]com	C2 domain
domain	updatamail[.]kozow[.]com	C2 domain
domain	updatasuccess[.]ddnsgeek[.]com	C2 domain
domain	updateservices[.]kozow[.]com	C2 domain
domain	updatetools[.]giize[.]com	C2 domain
domain	uscplxsecjs[.]ddnsgeek[.]com	C2 domain
domain	usoshared1[.]ddnsfree[.]com	C2 domain
domain	vals[.]bumbleshrimp[.]com	C2 domain
domain	vass[.]ooguy[.]com	C2 domain
domain	vass2025[.]casacam[.]net	C2 domain
domain	vmtools[.]camdvr[.]org	C2 domain
domain	vmtools[.]loseyourip[.]com	C2 domain
domain	vosies[.]ddnsfree[.]com	C2 domain
domain	vpaspmine[.]freeddns[.]org	C2 domain
domain	wdlcamaakc[.]ooguy[.]com	C2 domain

domain	winfoss1[.]kozow[.]com	C2 domain
domain	ysiohbk[.]camdvr[.]org	C2 domain
domain	zammffayhd[.]ddnsfree[.]com	C2 domain
domain	zmcmvmbm[.]ddnsfree[.]com	C2 domain
domain	zwmn350n3o1fsdf3gs[.]kozow[.]com	C2 domain
domain	zwmn350n3o1ugety2xbe[.]camdvr[.]org	C2 domain
domain	zwmn350n3o1vsdrggs[.]ddnsfree[.]com	C2 domain
domain	zwt310n3o1unety2kab[.]webredirect[.]org	C2 domain
domain	zwt310n3o2unety6a3k[.]kozow[.]com	C2 domain
domain	zwt31n3t0nidoqmve[.]camdvr[.]org	C2 domain
domain	zwt3ln3t1aimckalw[.]theworkpc[.]com	C2 domain
url	http://130.94.6.228/apt.tar.gz	Archive downloaded from 130.94.6[.]228. Contained GRIDTIDE.
url	http://130.94.6.228/amp.tar.gz	Additional archive downloaded. Contained hamcore.se2, a SoftEtherVPN Bridge component.
url	http://130.94.6.228/update.tar.gz	Additional archive downloaded. Contained vmlog (renamed to fire), a SoftEtherVPN Bridge component.
file	d25024ccea8eac85a9522289cfb709f2ed4e20176dd37855bacc2cd75c995606	Self-signed X.509 SSL certificate
file	01fc3bd5a78cd59255a867ffb3dfdd6e0b7713ee90098ea96cc01c640c6495eb	Key file used by GRIDTIDE to decrypt its Google Drive configuration.
file	669917bad46a57e5f2de037f8ec200a44fb579d723af3e2f1be1e8479a267966	SoftEtherVPN Bridge configuration.
file	ce36a5fc44cbd7de947130b67be9e732a7b4086fb1df98a5afd724087c973b47	GRIDTIDE
file	eb08c840f4c95e2fa5eff05e5f922f86c766f5368a63476f046b2b9dbffc2033	Malicious systemd service file created for GRIDTIDE persistence.

Annex B - MITRE ATT&CK Tactics and Techniques

Tactic	Technique ID	Remarks
Initial Access	T1133 – External Remote Services	Gains access via exposed remote services (for example, VPN, SSH, or management interfaces).
Execution	T1059.004 – Command and Scripting Interpreter: Unix Shell	Uses bash/sh shells to run commands and scripts on Linux hosts.
	T1059.009 – Command and Scripting Interpreter: Cloud API	Invokes cloud or provider APIs to execute actions remotely.
	T1064 – Scripting	Executes scripts to automate tasks and run malicious logic.
	T1106 – Native API	Calls native OS or platform APIs directly for execution.
	T1569.002 – System Services: Service Execution	Starts or restarts services to execute attacker-controlled binaries.
	T1569.003 – System Services: Systemctl	Uses systemctl to manage services for running or persisting malware.
Persistence	T1133 – External Remote Services	Maintains ongoing access through valid remote service credentials.
	T1543.002 – Create or Modify System Process: Systemd Service	Creates or modifies systemd service units for persistence on Linux systems.
Privilege Escalation	T1055 – Process Injection	Injects code into other processes to run with higher privileges or evade detection.
	T1543.002 – Create or Modify System Process: Systemd Service	Configures systemd services to run with elevated privileges.
Defense Evasion	T1027 – Obfuscated Files or Information	Obfuscates code, scripts, or configuration to evade detection.
	T1036 – Masquerading	Makes files, processes, or services appear legitimate through naming and metadata.
	T1055 – Process Injection	Injects into benign processes to hide malicious activity.
	T1064 – Scripting	Uses scripts to blend malicious actions with administrative activity.
	T1140 – Deobfuscate/Decode Files or Information	Decodes or unpacks payloads at runtime to hinder static analysis.
	T1222.002 – File and Directory Permissions	Adjusts POSIX permissions to protect or hide malicious components.

	Modification: Linux and Mac	
	T1497 – Virtualization/Sandbox Evasion	Detects or evades virtualized and sandboxed analysis environments.
	T1564.001 – Hide Artifacts: Hidden Files and Directories	Hides files or directories to avoid user and tool visibility.
	T1564.011 – Hide Artifacts: Ignore Process Interrupts	Configures processes to ignore interrupts or signals to resist termination.
Credential Access	T1003.008 – OS Credential Dumping: /etc/passwd and /etc/shadow	Targets Linux password and shadow files to obtain account hashes.
Discovery	T1016.001 – System Network Configuration Discovery: Internet Connection Discovery	Tests outbound connectivity and available egress paths.
	T1016 – System Network Configuration Discovery	Enumerates network interfaces, routes, and DNS settings.
	T1033 – System Owner/User Discovery	Identifies the currently logged-in user and local accounts.
	T1049 – System Network Connections Discovery	Lists active network connections to identify services and peers.
	T1057 – Process Discovery	Enumerates running processes to find security tools and targets.
	T1082 – System Information Discovery	Collects OS, hardware, and environment details.
	T1083 – File and Directory Discovery	Searches the filesystem for interesting data or locations.
	T1087 – Account Discovery	Enumerates local or domain accounts for further access.
	T1497 – Virtualization/Sandbox Evasion	Uses checks to determine if the host is virtualized or sandboxed.
	T1518.001 – Software Discovery: Security Software Discovery	Identifies installed security products and monitoring tools.
Lateral Movement	T1021.004 – Remote Services: SSH	Uses SSH for interactive access and lateral movement between systems.
Collection	T1074 – Data Staged	Aggregates collected data into local staging locations.

	T1560 – Archive Collected Data	Compresses and archives data before exfiltration.
Command and Control	T1071.001 – Application Layer Protocol: Web Protocols	Uses HTTP/HTTPS as the primary C2 channel to blend with normal web traffic.
	T1102 – Web Service	Leverages web services or APIs as C2 relays or data dead drops.
	T1105 – Ingress Tool Transfer	Transfers additional tools and payloads into compromised hosts.
	T1132.002 – Data Encoding: Non-Standard Encoding	Uses custom or uncommon encodings to hide C2 or exfiltrated data.
	T1572 – Protocol Tunneling	Tunnels C2 traffic inside other protocols to evade controls.
	T1573.002 – Encrypted Channel: Asymmetric Cryptography	Uses asymmetric encryption (for example, TLS) to secure C2 communications.
Resource Development	T1583.003 – Acquire Infrastructure: Virtual Private Server	Threat actor acquires VPS infrastructure to host C2 and staging servers.
	T1587.003 – Develop Capabilities: Digital Certificates	Develops or customizes digital certificates for secure C2 and impersonation.
	T1608.003 – Stage Capabilities: Install Digital Certificate	Installs crafted certificates on attacker-controlled systems to support malicious operations.

Annex C – YARA Rule for GRIDTIDE

```
rule Backdoor_GRIDTIDE {
        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 22 4A 57 54 22 7D 00 }
                $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 ($*)
}
```

References

1. Exposing the Undercurrent: Disrupting the GRIDTIDE Global Cyber Espionage Campaign

2. Cyberspies breached dozens of telecom firms, govt agencies

3. Google Disrupts Hackers Targeting Telecoms, Governments