2026 HACKER CALENDAR:

Advanced Persistent Threat edition

Cyber threats illustrated

Illustrations by Dan Borges

BLAZE

INFORMATION SECURITY

The illustrations are meant to raise awareness about the tactics, techniques and procedures of currently active threat actors and APT groups. This publication does not intend to glamorize or support any cybercriminal groups, nations, ideologies, or individuals. Don't do crimes. Be excellent to each other.

Cozy Bear/Midnight Blizzard/APT29

Russia — Espionage

Targets: Tech/SaaS · gov · NGOs · EU/US/JP

TTP: OAuth/tenant abuse; password spraying; mailbox delegation; cloud-blended C2.

JANUARY

sun	mon	tue	wed	thu	fri	sat
				01 New Year's Day	02	03
04	05	06	07	08	09	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24 DistrictCon (Washington, DC)
25 DistrictCon (Washington, DC)	26	27	28	29	30	31

Mustang Panda/RedDelta/TA416

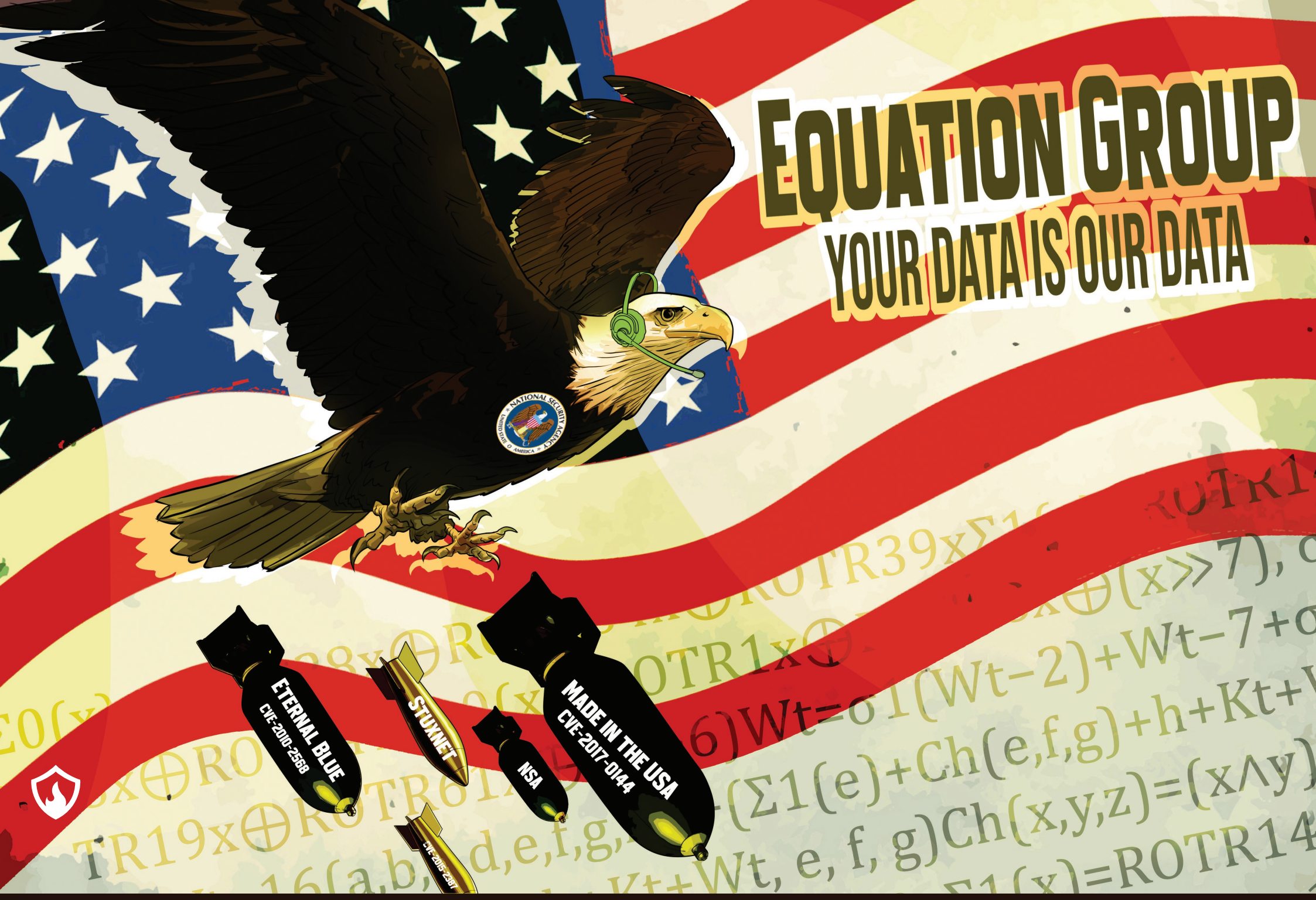
China — Espionage

Targets: Gov · NGOs · policy/think tanks · EU/SE Asia

TTP: Spear-phishing; DLL sideloading; StarProxy/ToneShell; PlugX.

FEBRUARY

sun	mon	tue	wed	thu	fri	sat
01	02	03	04	05	06	07
08	09	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28



Equation Group/EQGRP

United States of America — Espionage

Targets: Gov/defense · telecom · energy · research · ME/Asia/Global

TTP: Supply-chain interdiction; zero-days; removable-media worms; firmware/bootkits; HDD-level persistence.

MARCH

sun	mon	tue	wed	thu	fri	sat
01	02	03	04	05	06	07
08	09	10	11	12	13	14
15	16	17	18	19	20	21 BSides SF (USA)
22 BSides SF (USA)	23 RSA Conference (San Francisco)	24 RSA Conference (San Francisco)	25 RSA Conference (San Francisco)	26 RSA Conference (San Francisco)	27	28
29	30	31				

Volt Typhoon/Vanguard Panda

China — Pre-positioning & espionage

Targets: Critical infrastructure · US/Five Eyes

TTP: Edge-device footholds; LOTL; router/proxy chains; minimal malware, long-term access.

APRIL

sun	mon	tue	wed	thu	fri	sat
			01	02	03	04
05 Easter	06	07	08	09	10	11
12	13	14	15	16	17	18
19	20	21 Black Hat Asia 2026 (Singapore)	22 Black Hat Asia 2026 (Singapore)	23 Black Hat Asia 2026 (Singapore)	24	25
26	27	28	29	30		

Lazarus/TraderTraitor cluster

North Korea — Financial theft & espionage

Targets: Crypto/DeFi · software vendors · exchanges · finance/global

TTP: Dev/social engineering; trojanized apps; cross-platform loaders; wallet-key theft.

MAY

sun	mon	tue	wed	thu	fri	sat
					01	02
03	04	05	06	07	08	09
10	11	12	13	14	15 OffensiveCon 26 (Berlin)	16 OffensiveCon 26 (Berlin)
17	18	19	20	21 Ekoparty Miami 2026 (USA)	22 Ekoparty Miami 2026 (USA)	23
24	25	26	27	28	29	30
31						

Static Kitten/MuddyWater

Iran — Espionage

Targets: Telco · gov · oil & gas · IT services · ME/EU/NA

TTP: Spear-phish → PowerShell/LOTL; RMM (Atera/ScreenConnect); HTTP/DNS C2; faux-ransomware cover.

JUNE

sun	mon	tue	wed	thu	fri	sat
	01	02	03	04	05	06
07	08	09	10	11	12	13
14	15	16	17	18	19	20
21	22 OWASP Global AppSec EU (Vienna)	23 OWASP Global AppSec EU (Vienna)	24 OWASP Global AppSec EU (Vienna)	25 OWASP Global AppSec EU (Vienna)	26 OWASP Global AppSec EU (Vienna)	27
28	29	30				

Сандворт

Sandworm/Iridium/APT44

Russia/GRU Unit 74455 — Disruption & espionage

Targets: Energy · telecom · gov · UA/EU/US

TTP: Edge/supply-chain intrusion; AD/OT pivots; destructive wipers; multi-stage loaders.

JULY

sun	mon	tue	wed	thu	fri	sat
			01	02	03	04
05	06	07	08	09	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

Scattered Spider/Octo Tempest/UNC3944

United States/United Kingdom (non-state) — Financial extortion & intrusions

Targets: Tech/SaaS · telco · retail/hospitality · aviation · US/EU

TTP: Help-desk social engineering; SIM-swap/MFA resets; IdP/SSO abuse; RMM-based hands-on access.

AUGUST

sun	mon	tue	wed	thu	fri	sat
						01 Black Hat USA (Las Vegas)
02 Black Hat USA (Las Vegas)	03 Black Hat USA (Las Vegas)	04 Black Hat USA (Las Vegas)	05 Black Hat USA (Las Vegas)	06 Black Hat USA (Las Vegas) DEF CON 34 (Las Vegas)	07 DEF CON 34 (Las Vegas)	08 DEF CON 34 (Las Vegas)
09 DEF CON 34 (Las Vegas)	10	11	12	13	14	15
16	17	18	19	20	21	22
23 30	24 31	25	26	27	28	29

ShinyHunters

Multi-national (non-state) — Data theft & leaks

Targets: Consumer platforms · retail · tech startups · EU/Global

TTP: Credential phish/stuffing; repo/CI misconfig abuse; mass DB exfil; leak-site monetization.

SEPTEMBER

sun	mon	tue	wed	thu	fri	sat
		01	02	03	04	05
06	07	08	09	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26 BSides Krakow (Poland)
27	28	29	30			

Salt Typhoon/GhostEmperor

China — Telecom espionage

Targets: Mobile carriers · ISPs · satellite comms · US/EU/Global

TTP: Edge/network-gear compromise; LOTL; router proxy chains; long-term CDR/geolocation access.

OCTOBER

sun	mon	tue	wed	thu	fri	sat
				01	02	03
04	05	06	07	08	09	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Kimsuky/Velvet Chollima/Thallium

North Korea — Espionage & info ops

Targets: Policy think tanks · academia · defense/contractors · KR/US/EU

TTP: Tailored phishing → account takeover; reconnaissance-first ops; custom info-stealers.

NOVEMBER

sun	mon	tue	wed	thu	fri	sat
01	02	03	04	05	06	07
08	09	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30					

Fancy Bear/Forest Blizzard/APT28

Russia/GRU — Espionage

Targets: Gov · defense · education · EU/US

TTP: External exploits (incl. spooler-class); credential theft; HTTPS/webshell C2; LOLBins.

DECEMBER

sun	mon	tue	wed	thu	fri	sat
		01	02	03	04	05
06	07	08	09	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25 Christmas Day	26
27 Chaos Communication Congress (40C3) (Hamburg)	28 Chaos Communication Congress (40C3) (Hamburg)	29 Chaos Communication Congress (40C3) (Hamburg)	30 Chaos Communication Congress (40C3) (Hamburg)	31		