Raport eveniment cibernetic

APT

Unit 42 al Palo Alto a identificat infrastructura chineză APT asociată cu următorul certificat SSL malițios:

Subject Full Name	C=US,ST=Some-State,O=Internet Widgits Pty Ltd,CN=10.200.206.100
Issuer Full Name	C=US,ST=Some-State,O=Internet Widgits Pty Ltd,CN=COM
Serial Number	15007560845348164646
SHA1 Hash	B8CFF709950CFA86665363D9553532DB9922265C
Valid From	2017-11-23
Valid To	2027-11-21

Unit 42 a identificat că acest certificat SSL malițios a fost utilizat de servere localizate pe șase adrese IP specifice. Fiecare dintre aceste servere găzduiește multiple subdomenii asociate cu șase domenii distincte. Analiza denumirilor acestor domenii sugerează că unele dintre ele se prezintă ca servicii de stocare în cloud.

Această deghizare este probabil concepută pentru a oferi o aparență de legitimitate traficului intens și neobișnuit observat în perioadele de activitate sporită ale actorului malițios, cum ar fi în timpul exfiltrării de date din rețeaua victimei.

Informații sumare	
TIP	***Advenced Persistent threat***
IOC	
IP Adresa/Target port	• 165.232.186[.]197 / 80, 443, 4433 • 167.71.226[.]171 / 80, 81, 82, 443, 769, 4433, 8086, 8089 • 104.248.153[.]204 / 82, 443 • 143.110.189[.]141 / 443 • 172.105.34[.]34 / 8081, 8087, 8443, 8888 • 194.195.114[.]199 / 8080, 8443, 9200
Domene	• api.infinitycloud[.]info • connect.infinitycloud[.]info • ns.infinitycloud[.]info • connect.infinitybackup[.]net • ns1.infinitybackup[.]net • share.infinitybackup[.]net • file.wonderbackup[.]com • login.wonderbackup[.]com • sync.wonderbackup[.]com • update.wonderbackup[.]com • ads.teleryanhart[.]com • mfi.teleryanhart[.]com • dfg.ammopak[.]site • fwg.ammopak[.]site • jlp.ammopak[.]site • kwe.ammopak[.]site • lxo.ammopak[.]site • connect.clinkvl[.]com
Protecție și Mitigare	
	1. **Advanced URL Filtering**: Blochează solicitările web către URL-uri malițioase. Acest filtru analizează și blochează traficul web către URL-uri cunoscute ca fiind malițioase, împiedicând astfel accesul utilizatorilor și sistemelor la resurse potențial periculoase. 2. **DNS Security**: Previne eficient rezolvarea numelor de gazdă C2 (Command and Control). DNS Security detectează și blochează încercările de rezolvare a numelor de domeniu asociate cu infrastructura de comandă și control utilizată de atacatori, prevenind astfel comunicarea cu serverele malițioase. 3. **Container Runtime Inspection**: Previne solicitările DNS din procesele malițioase. Aceasta asigură monitorizarea și inspecția

solicitărilor DNS generate de procesele care rulează în containere, blocând acele solicitări care provin de la procese identificate ca fiind malițioase.

Resurse externe

	*https://unit42.paloaltonetworks.com/chinese-apt-linked-to-cambodia-government-attacks/*