Sinkholing Volatile Cedar DGA Infrastructure

By Kurt Baumgartner

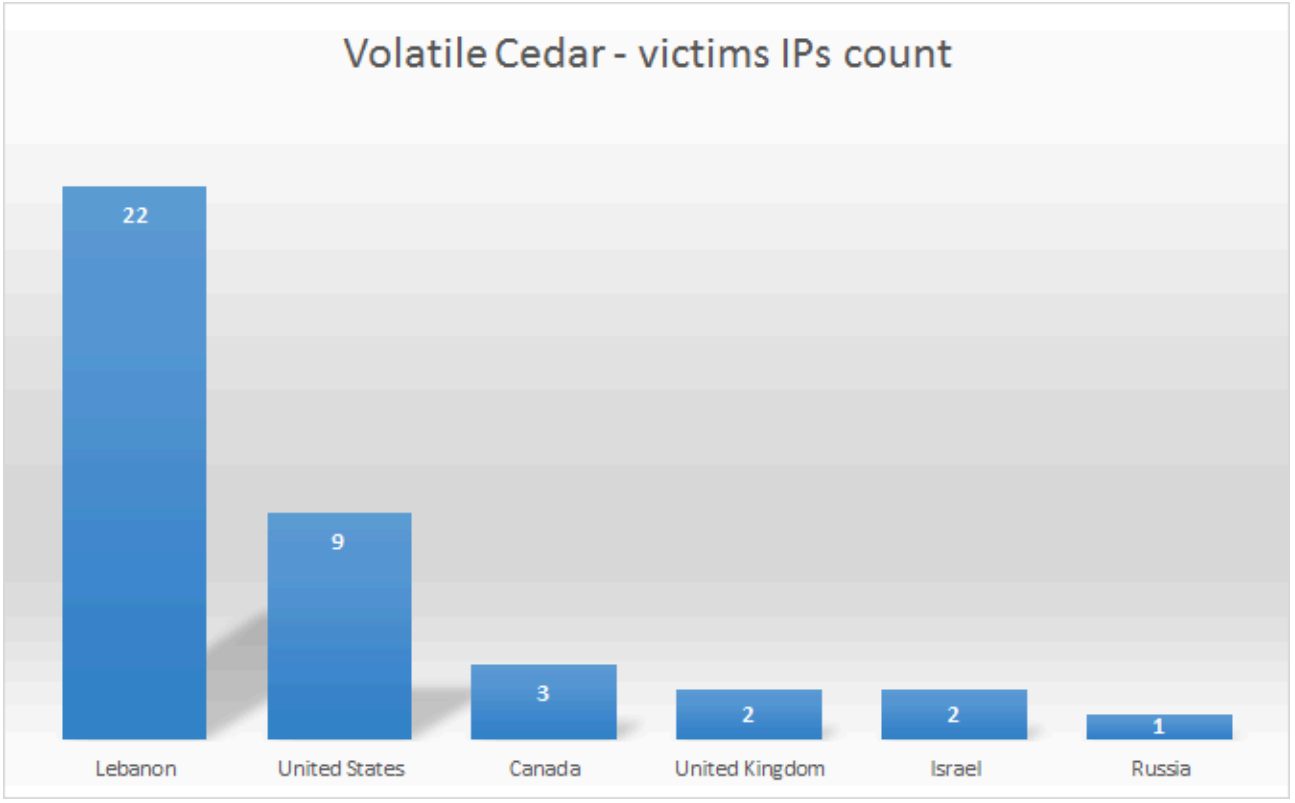
Published: 2015-03-31 · Archived: 2026-04-05 14:41:24 UTC

There is currently some buzz about the Volatile Cedar APT activity in the Middle East, a group that deploys not only custom built RATs, but USB propagation components, as reported by Check Point [pdf]. If you are interested in learning more about this APT, we recommend checking their paper first.

One interesting feature of the backdoors used by this group is their ability to first connect to a set of static updater command and control (C2) servers, which then redirect to other C2. When they cannot connect to their hardcoded static C2, they fall back to a DGA algorithm, and cycle through other domains to connect with.

Statistics:

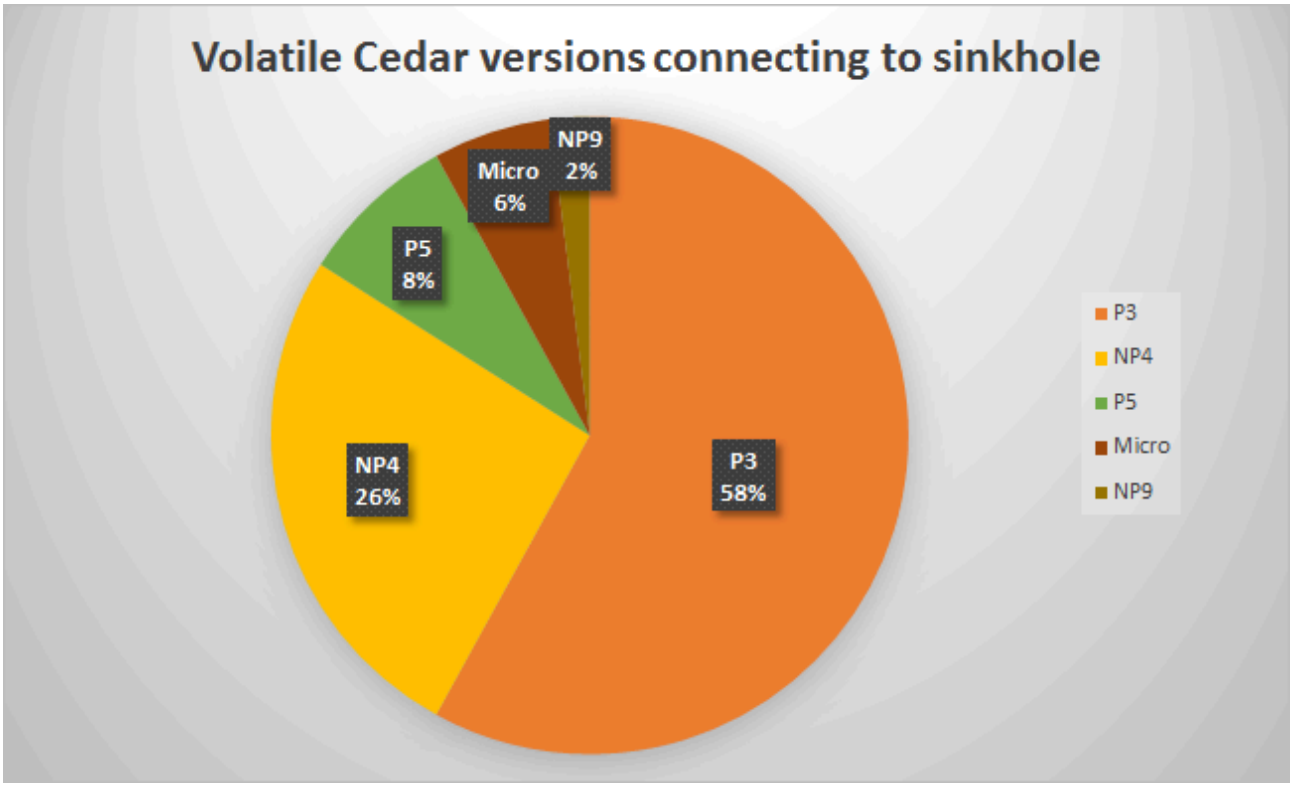
This particular actor's true impact seemed interesting, so we sinkholed some of their dynamically generated command and control infrastructure. These victim statistics present a somewhat surprising profile. Almost all of these victims are geolocated in Lebanon.



Victims checking in to DGA c2

Clearly, the bulk of the victims we observe are all communicating from ip ranges maintained by ISPs in Lebanon. And most of the other checkins appear to be research related. Almost all of the backdoors communicating with

sinkholed domains are the main “explosion” backdoor. But, some of the victim systems in Lebanon communicating with our sinkhole are running the very rare “micro” backdoor written up by our colleagues from Checkpoint in their paper: *“Micro is a rare Explosive version. It can best be described as a completely different version of the Trojan, with similarities to the rest of Explosive “family” (such as configuration and code base). We believe that Micro is actually an old ancestor of Explosive, from which all other versions were developed. As in other versions, this version is also dependent on a self-developed DLL named “wnhelp.dll.”* They check in to edortntexplore[.]info with the URI “/micro/data/index.php?micro=4” over port 443.



While Volatile Cedar certainly does not have a high level of technological prowess, it appears that they have been effective at spreading their malware, much like the Madi APT we reported on mid-2012. Because the group is not known for spearphishing, IT administrators should be aware of their own publicly exposed attack surface like web applications, ftp servers, ssh servers, etc, and ensure they are not vulnerable to SQLi, SSI attacks, and other server side offensive activity.

Kaspersky Verdicts and MD5s:

Trojan.Win32.Explosion.a
981234d969a4c5e6edea50df009efedd

Trojan.Win32.Explosion.b
7031426fb851e93965a72902842b7c2c

Trojan.Win32.Explosion.c
6f11a67803e1299a22c77c8e24072b82

Trojan.Win32.Explosion.d
eb7042ad32f41c0e577b5b504c7558ea

Trojan.Win32.Explosion.e
61b11b9e6baae4f764722a808119ed0c

Trojan.Win32.Explosion.f
c7ac6193245b76cc8cebc2835ee13532
184320a057e455555e3be22e67663722

Trojan.Win32.Explosion.g
5d437eb2a22ec8f37139788f2087d45d

Trojan.Win32.Explosion.i
7dbc46559efafe8ec8446b836129598c

Trojan.Win32.Explosion.j
c898aed0ab4173cc3ac7d4849d06e7fa

Trojan.Win32.Explosion.k
9a5a99def615966ea05e3067057d6b37

Trojan.Win32.Explosion.l
1dcac3178a1b85d5179ce75eace04d10

Trojan.Win32.Explosion.m
22872f40f5aad3354bbf641fe90f2fd6

Trojan.Win32.Explosion.n
2b9106e8df3aa98c3654a4e0733d83e7

Trojan.Win32.Explosion.o
08c988d6cebdd55f3b123f2d9d5507a6

Trojan.Win32.Explosion.p
1d4b0fc476b7d20f1ef590bcaa78dc5d

Trojan.Win32.Explosion.q
c9a4317f1002fefcc7a250c3d76d4b01

Trojan.Win32.Explosion.r
4f8b989bc424a39649805b5b93318295

Trojan.Win32.Explosion.s
3f35c97e9e87472030b84ae1bc932ffc

Trojan.Win32.Explosion.t
7cd87c4976f1b34a0b060a23faddbd19

Trojan.Win32.Explosion.u
ea53e618432ca0c823fafc06dc60b726

Trojan.Win32.Explosion.v
034e4c62965f8d5dd5d5a2ce34a53ba9

Trojan.Win32.Explosion.w
5ca3ac2949022e5c77335f7e228db1d8

Trojan.Win32.Explosion.x
ab3d0c748ced69557f78b7071879e50a

Trojan.Win32.Explosion.y
5b505d0286378efcca4df38ed4a26c90

Trojan.Win32.Explosion.z
e6f874b7629b11a2f5ed3cc2c123f8b6

Trojan.Win32.Explosion.aa
306d243745ba53d09353b3b722d471b8

Trojan.Win32.Explosion.ab
740c47c663f5205365ae9fb08adfb127

Trojan.Win32.Explosion.ac
c19e91a91a2fa55e869c42a70da9a506

Trojan.Win32.Explosion.ad
edaca6fb1896a120237b2ce13f6bc3e6

Trojan.Win32.Explosion.ae
d2074d6273f41c34e8ba370aa9af46ad

Trojan.Win32.Explosion.af
66e2adf710261e925db588b5fac98ad8
29eca6286a01c0b684f7d5f0bfe0c0e6
2783cee3aac144175fef308fc768ea63
f58f03121eed899290ed70f4d19af307

Trojan.Win32.Agent.adsct
826b772c81f41505f96fc18e666b1acd

Trojan-Dropper.Win32.Dycler.vhp
44b5a3af895f31e22f6bc4eb66bd3eb7

??
96b1221ba725f1aaeaaa63f63cf04092

References:

- Volatile Cedar – Analysis of a Global Cyber Espionage Campaign (Checkpoint)
