VOLATILE CEDAR

AXIAL

VOLATILE CEDAR

LEBANON

Canada, Israel, Lebanon, Russia, Sauc Arabia, UK, USA.

EXPLOSIVE

HAWK BASE
HOME FOR APT RESEARCHERS

AXIAL

A SURVEY ON VOLATILE CEDAR ABOUT, WEAPON OF CHOICE, TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. INTRODUCTION

Volatile Cedar also known as Dancing Salome is a threat group based out of Lebanon which focuses on information theft and espionage.

II. TARGETS

The target/s of this threat group mainly focuses on education, government, and hosting based services onto various countries like Canada, Israel, Lebanon, Russia, UK, USA.

.

III. METHODS USED

The methods used by this group used are various RATs, but USB propagation methods also they have been using a rare "micro" backdoor against their targets, also they have been using "Explosive" trojan to infect the victims, the trojan Explosive uses custom obfuscation techniques to various configuration values.

IV. CAMPAIGNS

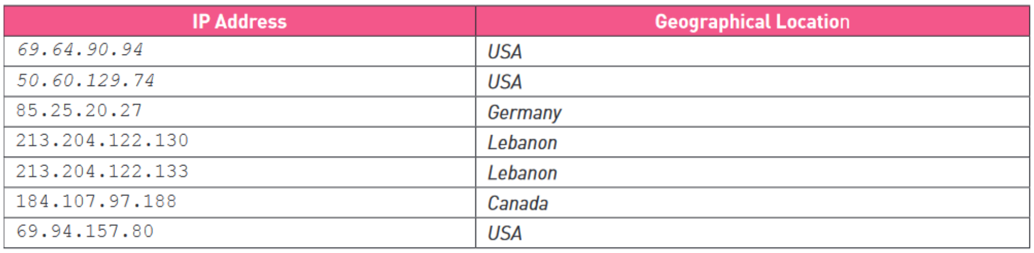
This threat group has been linked to campaigns related to attacks on individuals, companies and institutions worldwide around 2012, this same campaign was active for the next three years.

ATTRIBUTION

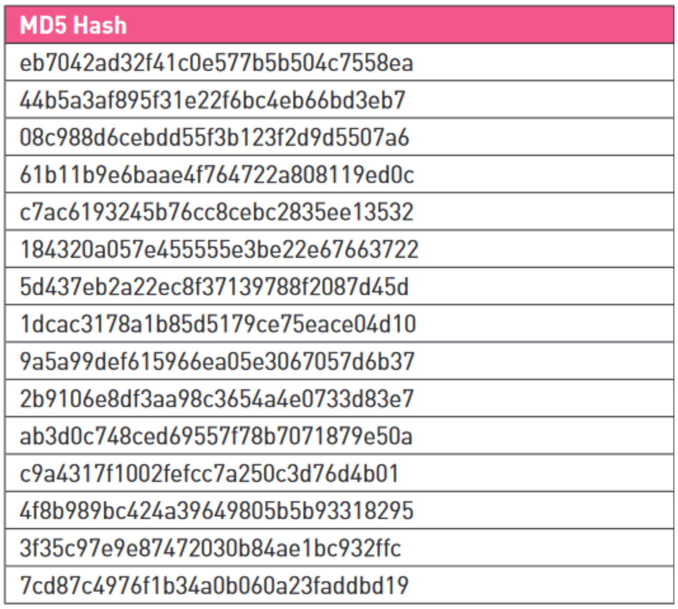
This threat group is attributed to be based out of Lebanon. The Trojan **Explosive** was hosted by a major Lebanese hosting company, DNS registrant information from these servers were previously registered under contacts with a very similar Lebanese address.

[Cited from Check Point Research]

V. IOCS



IP Address	Geographical Location
69.64.90.94	*USA*
50.60.129.74	*USA*
85.25.20.27	*Germany*
213.204.122.130	*Lebanon*
213.204.122.133	*Lebanon*
184.107.97.188	*Canada*
69.94.157.80	*USA*



MD5 Hash
eb7042ad32f41c0e577b5b504c7558ea
44b5a3af895f31e22f6bc4eb66bd3eb7
08c988d6cebdd55f3b123f2d9d5507a6
61b11b9e6baae4f764722a808119ed0c
c7ac6193245b76cc8cebc2835ee13532
184320a057e455555e3be22e67663722
5d437eb2a22ec8f37139788f2087d45d
1dcac3178a1b85d5179ce75eace04d10
9a5a99def615966ea05e3067057d6b37
2b9106e8df3aa98c3654a4e0733d83e7
ab3d0c748ced69557f78b7071879e50a
c9a4317f1002fefcc7a250c3d76d4b01
4f8b989bc424a39649805b5b93318295
3f35c97e9e87472030b84ae1bc932ffc
7cd87c4976f1b34a0b060a23faddbd19

Cited from CheckPoint

VI. REFRENCES

https://apt.thaicert.or.th/cgi-bin/showcard.cgi?g=Volatile%20Cedar

Check Point Research on Volatile Cedar