Volatile Cedar – Analysis of a Global Cyber Espionage Campaign

blog.checkpoint.com/2015/03/31/volatilecedar/

March 31, 2015

Today, we announced the discovery of Volatile Cedar, a persistent attacker group originating possibly in Lebanon with political ties.

Beginning in late 2012, the carefully orchestrated attack campaign we call *Volatile Cedar* has been targeting individuals, companies and institutions worldwide. This campaign, led by a persistent attacker group, has successfully penetrated a large number of targets using various attack techniques, and specifically, a custom-made malware implant codenamed *Explosive*. This report provides an extended technical analysis of *Volatile Cedar* and the *Explosive* malware.

Malware attribution is often tricky and deception-prone. With that in mind, investigation of the evidence leads us to suspect *Volatile Cedar* originates from Lebanon (hence its nickname). Moreover, the *Volatile Cedar* target vertical distribution strongly aligns with nation-state/political-group interests, eliminating the possibility of financially motivated attackers.

We have seen clear evidence that *Volatile Cedar* has been active for almost 3 years. While many of the technical aspects of the threat are not considered “cutting edge”, the campaign has been continually and successfully operational throughout this entire timeline, evading detection by the majority of AV products. This success is due to a well-planned and carefully managed operation that constantly monitors its victims’ actions and rapidly responds to detection incidents.

Volatile Cedar is heavily based on a custom-made remote access Trojan named *Explosive,* which is implanted within its targets and then used to harvest information. Tracking down these infections was quite a difficult task due to the multiple concealment measures taken by the attackers. The attackers select only a handful of targets to avoid unnecessary exposure. New and custom versions are developed, compiled and deployed specifically for certain targets, and ”radio silence” periods are configured and embedded specifically into each targeted implant.

The modus operandi for this attacker group initially targets publicly facing web servers, with both automatic and manual vulnerability discovery. Once in control of a server, the attackers further penetrate the targeted internal network via various means, including manual online hacking as well as an automated USB infection mechanism.

In our report, we discuss the attack vectors and infection techniques used by the attack campaign as well as provide indicators that can be used to detect and remove the infection. We’ve provided some more basic information below.

For in-depth information, please view our media alert and technical report.

We would like to acknowledge the following people for their contribution to the research efforts leading to this report: Lead researcher Yaniv Balmas, Irena Damsky, Maya Horowitz, Assaf Krintza, Michael Shalyt, Shahar Tal, Ron Davidson and Rachel Teitz.

Volatile Cedar – The Facts

What is Volatile Cedar?

Volatile Cedar is an APT malware campaign first detected and investigated by Check Point.

Who are the attackers behind Volatile Cedar?

We have seen evidence which suggests the attacker group is based in Lebanon. Victim geography and verticals may indicate the interests of a government/political group.

Who was attacked?

Among the confirmed targets, we identified defense contractor firms, telecommunications and media companies, and educational institutions. We confirmed live infections in approximately 10 different countries, including the USA, Canada, UK, Turkey, Lebanon and Israel.

What technical measures are used in the Volatile Cedar campaign?

The attacker’s main tool is a custom malware implant codenamed ‘Explosive’ (named by the attackers). Additionally, we have found traces of common hacking tools such as vulnerability scanners, web shells and public exploit code.

Why is it named Volatile Cedar?

Volatile is a synonym for explosive, and the cedar is Lebanon's national emblem.

How long has Volatile Cedar been operational?

We have seen evidence of activity starting in early 2012, and it is still ongoing as of this writing.

What is Check Point doing to mitigate this threat?

Check Point has deployed software protections to all its customers against the technical indicators of this attack. Additionally, we are publishing a report which describes and examines the security risks involved.

Has Volatile Cedar been detected before?

Earlier versions of the Explosive implant have been heuristically classified as malicious by multiple AV products. Each detection has almost immediately been followed by the removal of the compromised tool and the creation of a new, undetected, version. This is further proof of the group's relatively high operational level.

Where did Check Point first detect Volatile Cedar?

Check Point detected the Explosive malware on a web server in a customer network.

What abilities does Explosive have?

The implant has both passive collection methods and on-demand capabilities. Once installed, the tool continuously runs a keylogger and a clipboard logger, which transmit the results to the C&C server. In addition, Explosive has a wide array of options that can be activated by a C&C command, including a variety of data theft and machine fingerprinting capabilities, stealth and self-destruction functions, proliferation options and a remote shell.

Finally, the creators of Explosive went to great lengths to assure operational stealth to protect against exposure, including memory usage monitoring, process listing etc.

Can Explosive cause damage?

The main threat is sensitive data theft and cyber espionage. The implant has built-in file deletion functionality as well as arbitrary code execution, making it possible for the attackers to inflict a lot of damage on an infected system.

How can I remove the Explosive malware?

The Check Point technical report indicates which elements to remove to mitigate the live malware infection. Note: As in any malware infection, the attackers may have obtained credentials or other methods of accessing to your network, which requires additional means of protection.

I have significant information about the campaign or its victims. Who do I contact?

We have opened the mailbox for information sharing purposes.