THE UNBEARABLE LIGHTNESS OF APTing
WHO ARE WE?

Ron Davidson
Head of Threat Intelligence and Research
Check Point Software Technologies

Yaniv Balmas
Security Researcher
Check Point Software Technologies
An **APT** is a network attack in which an unauthorized person gains access to a network and stays there undetected for a long period of time.
APT is a set of stealthy and continuous computer hacking processes ... APT usually targets organizations and/or nations for business or political motives.

"An APT is a network attack in which an unauthorized person gains access to a network and stays there undetected for a long period of time."
“APT is a set of stealthy and continuous computer hacking processes ... APT usually targets organizations and/or nations for business or political motives.”

“An APT is a network attack in which an unauthorized person gains access to a network and stays there undetected for a long period of time.”
WHAT’S COMMON?

Attribution

China
Iran
USA
Russia
Israel
DPRK

@AttributionDice
WHAT’S IN COMMON?

- China: 44%
- USA: 23%
- Russia: 9%
- Iran: 9%
- France: 11%
- Israel: 5%
WHEN IN DOUBT...

It’s probably China!
WITH GREAT POWER COME GREAT APTS
VOLATILE CEDAR

- A targeted campaign
- Has been active since late 2012
- Operation was terminated following our publication at March 2015
WHY VOLATILE CEDAR?

Explosive-443
TEL AVIV — Defense Minister Moshe Ya’alon confirmed Wednesday that Israel was the target of cyber attacks by Iran during last summer’s Gaza war and by Hezbollah, which reportedly ran an operation going back three years.

Speaking at an international cyber security conference at Tel Aviv University, Ya’alon insisted “no significant damage” was inflicted by Iranian operatives, terror organizations and hackers who targeted government, military and economic sites during the July-August 2014 Operation Protective Edge.

He confirmed for the first time findings from Tel Aviv-based Check Point Software Technologies, which reported to its clients in March that Israel, several Western countries and other Middle East states had since 2012 been targets of a sustained cyber spying campaign that the company believed was run out of Lebanon.

At the time, Check Point did not specifically name Hezbollah as the culprit for the cyber spying campaign, which the company dubbed “Volatile Cedar.” It only noted that command-and-control servers supporting malware activities were traced to a hosting company in Lebanon, while several other servers were registered with “a very similar” Lebanese address. According to the cyber security and information technology firm, the campaign was based on Trojan horse computer malware planted in its targets, which was activated to collect data over extended periods.

“Monitoring these cyber infections was very challenging, due to the numerous ways in which they were disguised by the hackers,” the Check Point report noted.
HEZBOLLAH

- “Party of God”
- Islamist political and militant group
- Part of the Lebanese government
- Funded by Iran
- Official flag contains an AK-47
HEZBOLLAH

- “Party of God”
- Islamist political and militant group
- Part of the Lebanese government
- Funded by Iran
- Official flag contains an AK-47
PERSISTENT

Version 1
Version 2
KS Version
Micro Version
Version 3

Nov 12  Mar 13  July 13  Nov 13  Mar 14  July 14  Nov 14
TARGETS

• Targets were carefully chosen.
Targets were carefully chosen.

Very specific geopolitical sector.

- Israel: Number of Detected Infections: 232
- Lebanon: Number of Detected Infections: 158
- Saudi Arabia: Number of Detected Infections: 60
• Targets were carefully chosen.

• Very specific geopolitical sector.

• Malicious activity was mostly key-logging and clip-board logging.
ADVANCED?!  

I can has 72 virgins
ADVANCED?! VS

Keith B. ALEXANDER VS Hassan NASRALLAH
Round 1

ATTACK VECTOR
STUXNET

Attack Vector

- Deliver USB drives into a super secured site
- USB Contains 4 0-days
- CPLink vulnerability
- Lateral movement via peer to peer RPC
The target itself might be a hard nut to crack.

Look in its proximity…

Exploit default un-patched IIS installations.

Insert a web-shell and a key-logger into compromised servers.

Use key-logging data for lateral movement.
Round 2

PERSISTENCE
**EQUATION**

**Persistence**

- Insert implant code into hard-drive firmware
- Support 12 different HDD vendors/variations
- Possibly infect boot sector
VOLATILE CEDAR

Persistence

- Install as a new service
- What if service gets removed\stopped?
- Use web-shell to restart\reinstall it
Round 3
COMMAND AND CONTROL
PLUGX

Command & Control

- Victim-side C&C servers are legit hosts
- A custom DNS resolver is used by the malware
- This DNS is hijacked and redirects to the C&C server
VOLATILE CEDAR

Command & Control

- “Advanced” DGA Algorithm
- Command & Control
VOLATILE CEDAR

Command & Control

- “Advanced”
VOLATILE CEDAR

- “Advanced” DGA Algorithm
- Use hijacked sites & cheap VPS as infrastructure

~753250 LBP

~500$
Round 4
STEALTH
REGIN

Stealth

• Six stage architecture.
• Use both user-land code and kernel modules.
• Store stages in a custom Virtual File System.
REGIN

- Six stage architecture
- Use both user land code and kernel modules.
- Store stages in a custom Virtual File System.
**Stealth**

- Create a dedicated thread to monitor process CPU activity.
- Once CPU usage is greater than the threshold
- Restart the process ;)

**VOLATILE CEDAR**
Round 5

ENCRYPTION
Encryption

- Usage of AES, RC5 and RC6
- A unique RC6 implementation designed for better performance.
VOLATILE CEDAR

Encryption

- Reversed Strings.

google.com → moc.elgoog
VOLATILE CEDAR

Encryption

- Reversed Strings.
- Oh, wait… That might be too easy to spot
- Use Base-64!

`google.com` → `moc.elgoog` → `bW9jLmVsZ29vZW==`
• Reversed Strings.
• Oh, wait… That might be too easy to spot
• Use Base-64!
• Oh no, now it looks like Base-64.

```
google.com  →  moc.elgoog  →  bW9jLmVsZ29vZw==
```
VOLATILE CEDAR

Encryption

• Reversed Strings.
• Oh, wait… That might be too easy to spot
• Use Base-64!
• Oh no, now it looks like Base-64.

google.com ➔ moc.elgoog ➔ bW9jLmVsZ29vZw== ➔ ==wZv92ZsVmlj9Wb
CONCLUSIONS

• “Advanced” is a very subjective term

• Dedication can sometimes be as effective as resources

• APT is no longer the sole domain of multi-billion dollar organizations.
MORE RECENT EXAMPLES

• The Spy Kittens Are Back: Rocket Kitten 2
  - Cedric Pernet - Trend Micro
  - Eyal Sela - ClearSky
ROCKET KITTEN 2

Threat?

“We believe the espionage factor and political context make their attacks unique and very different from traditional targeted attacks... This is an obvious case of politically inspired or motivated espionage.”

“550 Targets, most of which are located in the Middle East... policy research, diplomacy, all aspects of international affairs, defense, security, journalism, human rights... Israeli academic institution... scientists, journalists, researchers, and sometimes expatriated Iranians living in Western countries...”
ROCKET KITTEN 2

Persistent?

“Numerous attempts to attack the same (chosen) targets for as long as necessary”

“Barrage targets until they eventually slip”

“The attackers do make up for these disadvantages with persistence...”
ROCKET KITTEN 2

Advanced?

“Simple tools and lack of professionalism... they don’t seem to put much effort into quality.

“The group is not very technically sophisticated... analysis of their code showed deficits and mistakes that a professional cybercriminal would not make... actors used off-the-shelf and low-quality tools.”
MWI AS AN APT TOOL

• A new Word Document Exploit Kit
  - Art Villeneuve, Joshua Homan, Fireeye
  - “advertised as an “APT” tool to be used in targeted attacks”

• Microsoft Word Intruder RTF Sample Analysis
  - Omni Herscovici, Check Point

• Microsoft Word Intruder Revealed
  - Gabor Szappanos, SophosLabs Hungary
MWI CAMPAIGN TARGETS

- Ministry of Education
- The Municipalities Computation Center
- The Social Security Authority
- Medical Centers
- An airline Carrier
- Government Export Agency
- The Supreme Court Network
- Government Aviation Authority
- A university computation center
THANK YOU!

rond@checkpoint.com
yanivb@checkpoint.com  @ynvb