New Data: Volatile Cedar Malware Campaign

blog.checkpoint.com/2015/06/09/new-data-volatile-cedar/

June 9, 2015

At the end of March, we published a blog post and a whitepaper about a cyber-espionage campaign dubbed “Volatile Cedar.” This campaign has successfully penetrated targets world-wide, using a variety of attack techniques, in particular, a custom-made malware implant codenamed *Explosive*.

Let’s recap what we know:

The Campaign:

- The Volatile Cedar operation has been active since 2012 and has evaded detection by the majority of AV products. Volatile Cedar constantly monitors its victims’ actions and rapidly responds to detection incidents.
- *Explosive* is a specially crafted Trojan type of malware, implanted in targets and used to harvest information. New and custom versions are developed, compiled and deployed for specific targets.
- The primary goal of the attackers appears to be data collection, not to cause harm to targets/use their resources or steal financial assets.

The Targets:

- Only a small number (hundreds as opposed to thousands) of targets have been identified to date. We would normally expect that a cyber-crime campaign targeting financial institutions would result in much higher numbers of victims. The limited number of targets may be part of an attempt to avoid unnecessary exposure.
- Identified targets are organizations in the fields of telecommunications, media, web hosting, academia, defense contractors and civil services.

All of these points indicate a highly crafted operation directed at specific and carefully selected targets.

Something Old, Something New

After going public with our findings, we were provided with a new configuration belonging to a newly discovered sample we have never seen before.

The sample itself is the same Explosive v3.0 implant, but it differs in the following aspects:

- A different DGA seed is used (flashplayergetadobe) to create new C2 servers. The only one we have noted so far is registered by the operators as “getadobeflashplayer[.]net”

- All of the victims of this thread are Saudi Arabia-based.

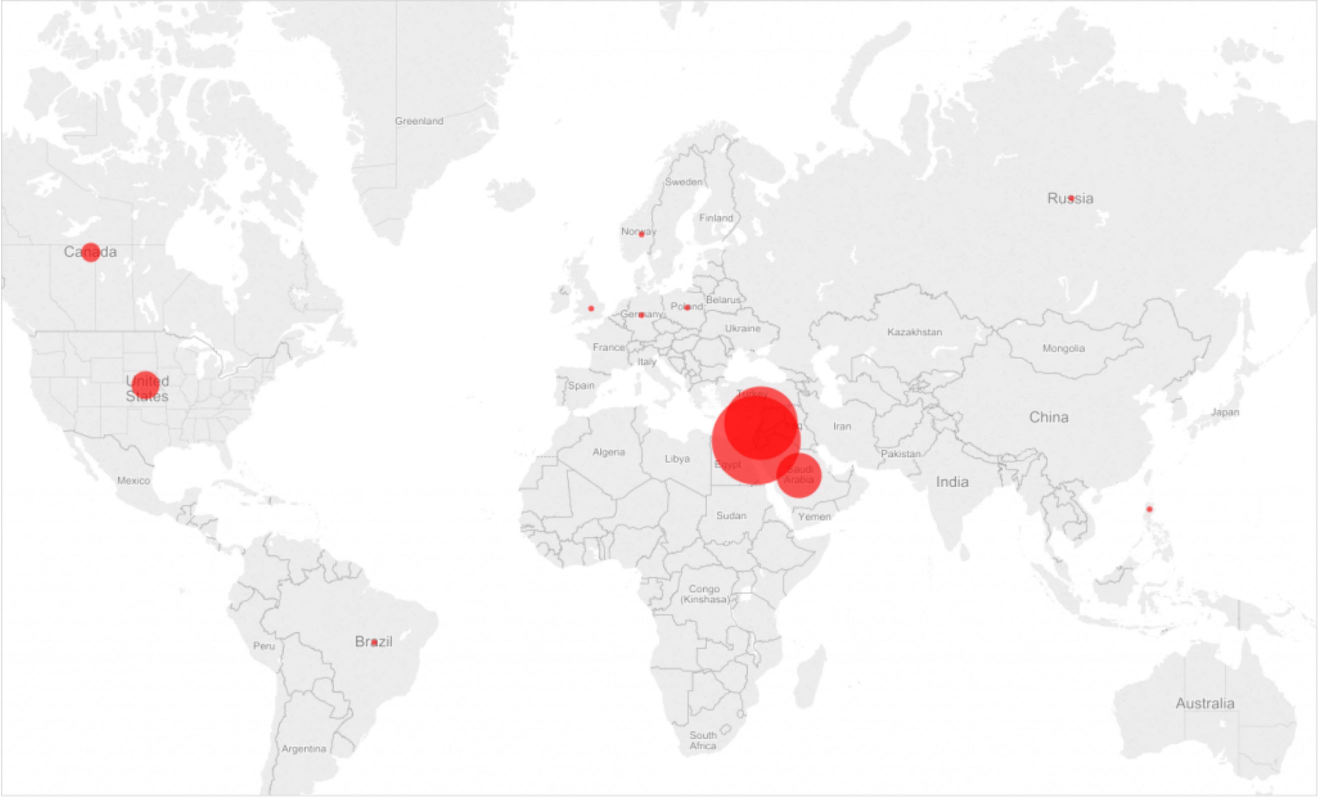
Attribution

We want to present our attribution case with stronger evidence to back up our claims and provide a more detailed explanation.

There were many questions raised by our colleagues and customers as to how and why we came to the conclusion that this operation originated in Lebanon.

Through careful analysis of the operation, both previously known victims and C2 servers as well as targets infected with the sample containing the newly discovered configuration, we were able to create a heat map of the infections.

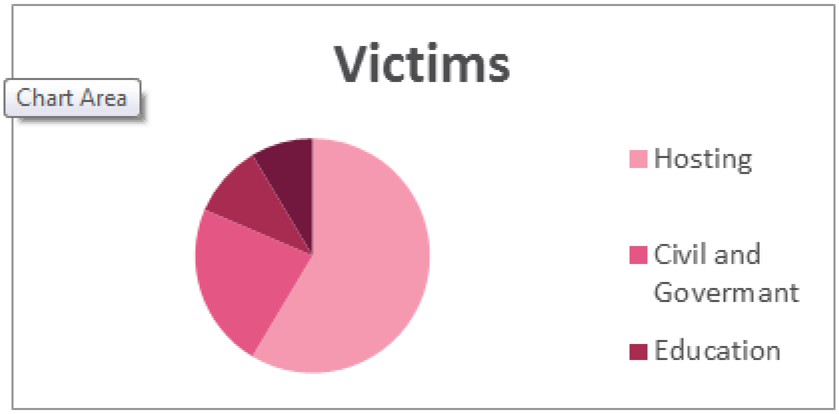
Looking at the target map of the operation we see the following:



Although there are infections all over the world, the highest concentration of infections is in the Middle East – specifically in Israel, Lebanon and Saudi Arabia.

So why do we still say that the group behind Volatile Cedar is Lebanese?

If we take a closer look at the targets, we see the distribution of the victims themselves based on industry vertical:



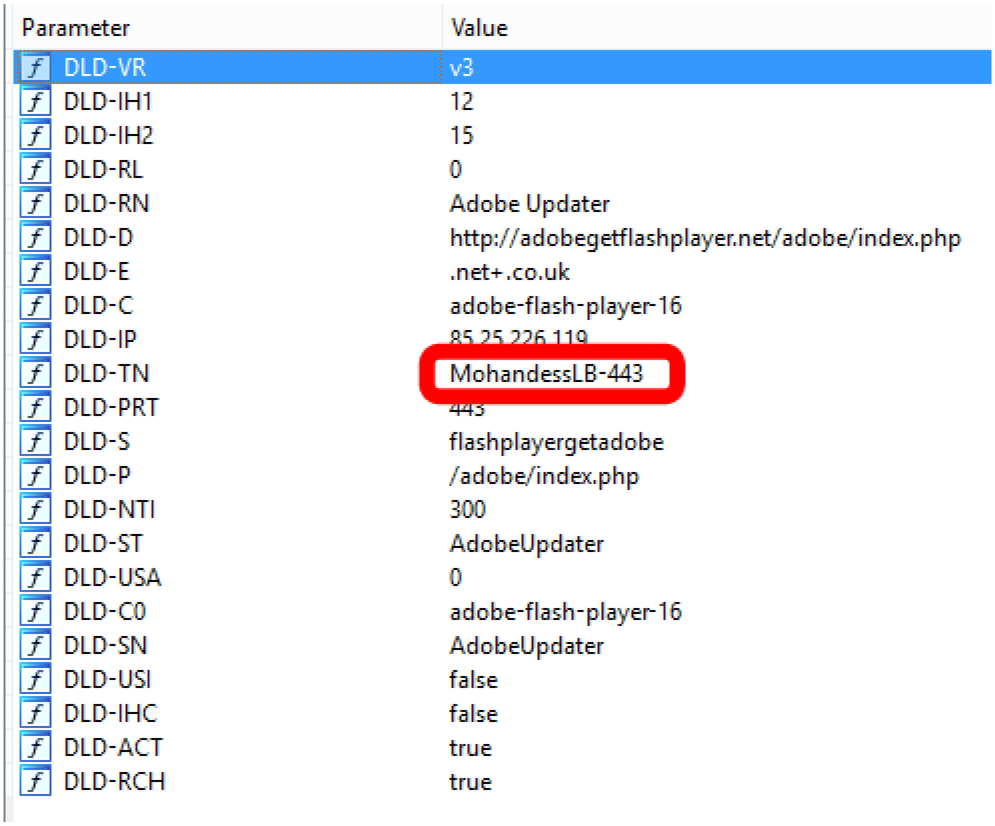
If we dig deeper and look into the distribution of the hacked websites on the hosting services, we notice the following two interesting facts:

1. The victim sites on the compromised web services were primarily Middle Eastern web sites. This is true not only for the majority of the infections in Israel, Lebanon and Saudi Arabia, but all over the world as well.
2. The majority of the victimized sites themselves belong to different companies that work with national and defense companies.

These observations about the victims allow us to assume that the operators behind this activity maintain high interest in the region and its politics.

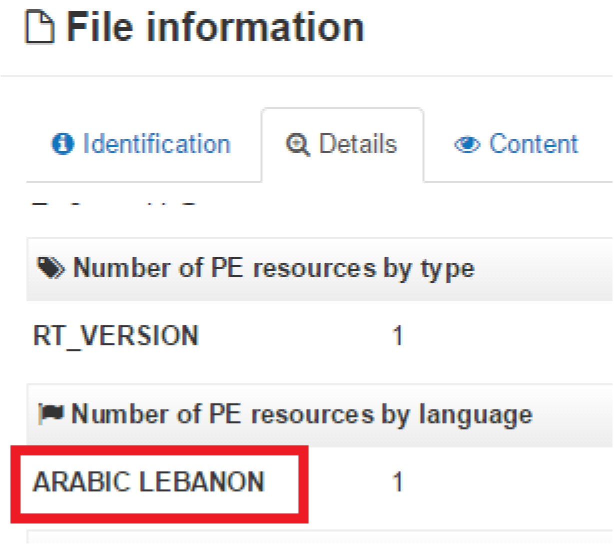
Other indications we found about the operators:

The strings inside the binary code in Arabic:



Parameter	Value
DLD-VR	v3
DLD-IH1	12
DLD-IH2	15
DLD-RL	0
DLD-RN	Adobe Updater
DLD-D	http://adobegetflashplayer.net/adobe/index.php
DLD-E	.net+.co.uk
DLD-C	adobe-flash-player-16
DLD-IP	85.25.226.119
DLD-TN	MohandessLB-443
DLD-PRT	443
DLD-S	flashplayergetadobe
DLD-P	/adobe/index.php
DLD-NTI	300
DLD-ST	AdobeUpdater
DLD-USA	0
DLD-C0	adobe-flash-player-16
DLD-SN	AdobeUpdater
DLD-USI	false
DLD-IHC	false
DLD-ACT	true
DLD-RCH	true

The PE resources inside the malware files are in Lebanese Arabic

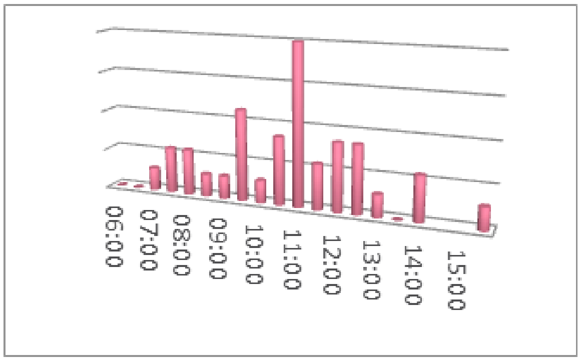


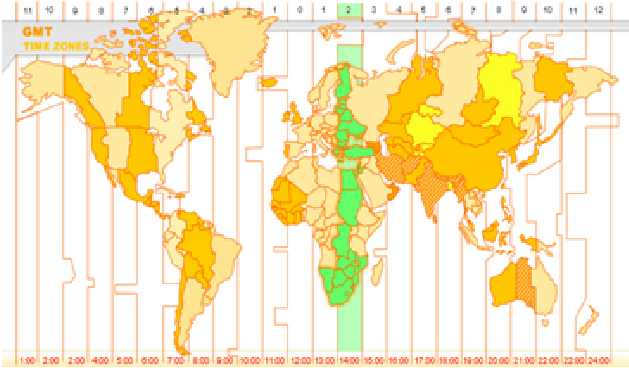
File information

Number of PE resources by type	
RT_VERSION	1

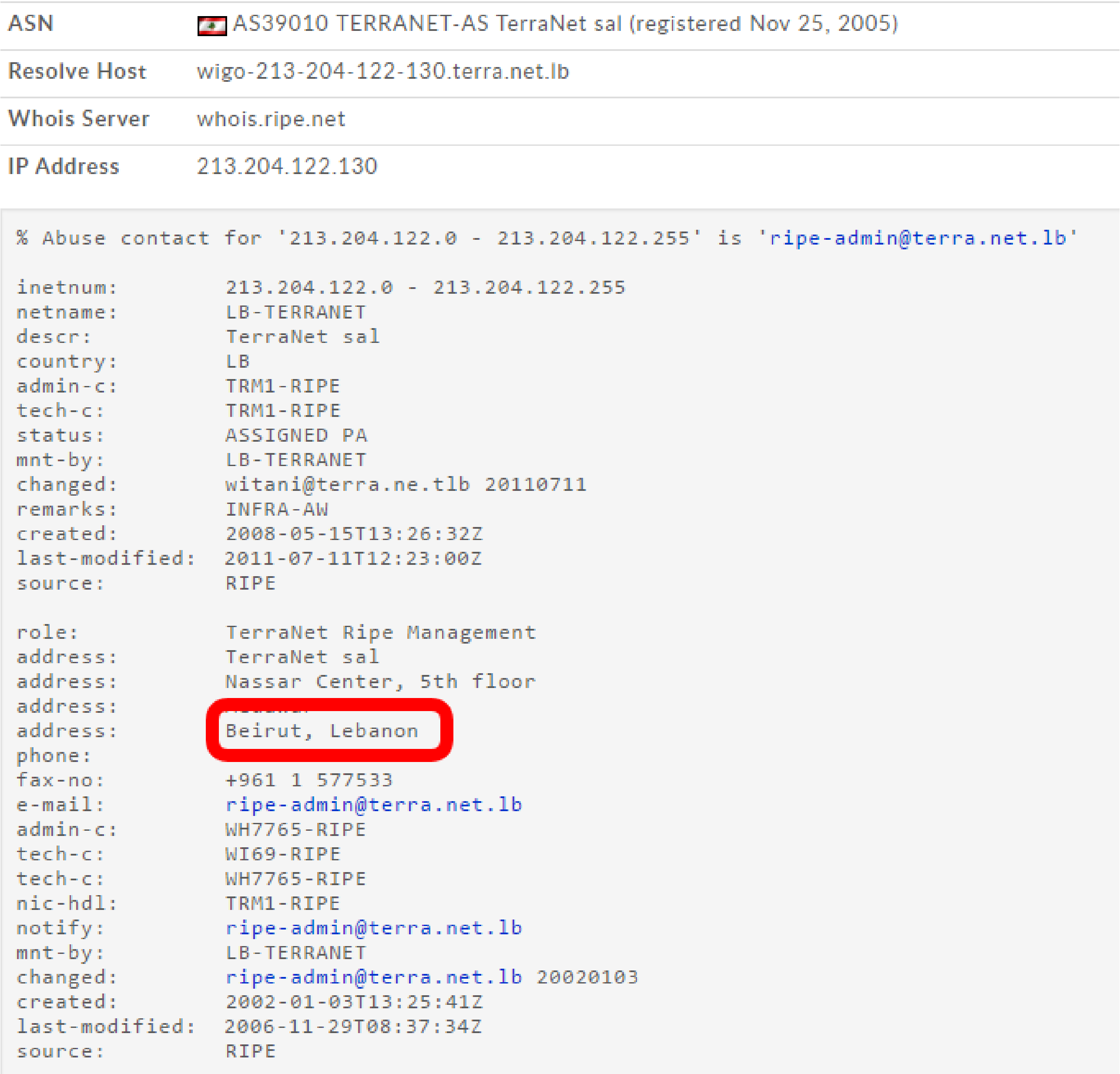
Number of PE resources by language	
ARABIC LEBANON	1

Compilation times – The time stamps correlate to the working hours of the Lebanese time zone (GMT+ 2).





Some of the C2 servers are hosted in Lebanon (true for the first *Explosive* version).



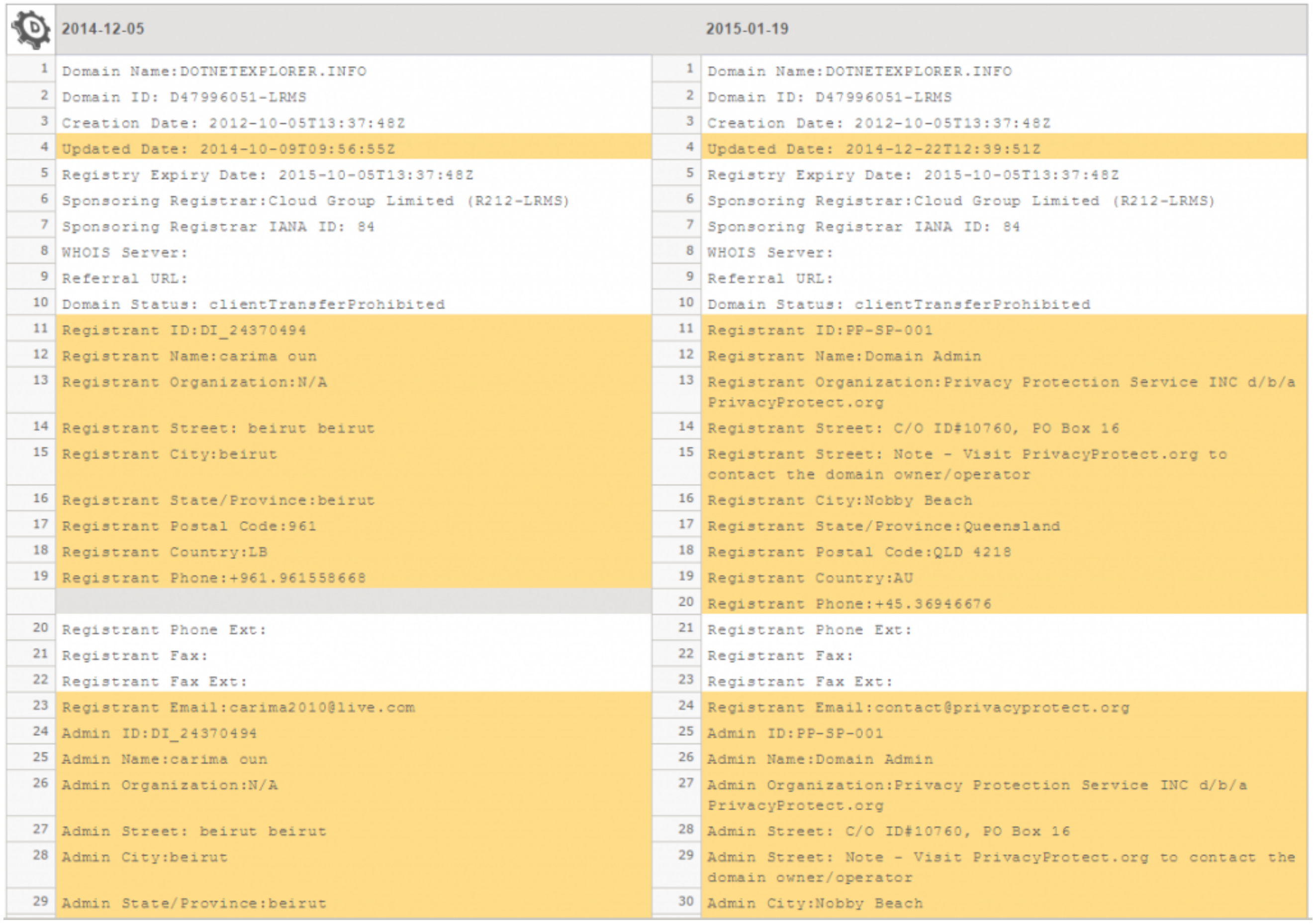
ASN	AS39010 TERRANET-AS TerraNet sal (registered Nov 25, 2005)
Resolve Host	wigo-213-204-122-130.terra.net.lb
Whois Server	whois.ripe.net
IP Address	213.204.122.130

```
% Abuse contact for '213.204.122.0 - 213.204.122.255' is 'ripe-admin@terra.net.lb'

inetnum:        213.204.122.0 - 213.204.122.255
netname:        LB-TERRANET
descr:          TerraNet sal
country:        LB
admin-c:        TRM1-RIPE
tech-c:         TRM1-RIPE
status:         ASSIGNED PA
mnt-by:         LB-TERRANET
changed:        witani@terra.ne.tlb 20110711
remarks:        INFRA-AW
created:        2008-05-15T13:26:32Z
last-modified:  2011-07-11T12:23:00Z
source:         RIPE

role:           TerraNet Ripe Management
address:        TerraNet sal
address:        Nassar Center, 5th floor
address:
address:        Beirut, Lebanon
phone:
fax-no:         +961 1 577533
e-mail:         ripe-admin@terra.net.lb
admin-c:        WH7765-RIPE
tech-c:         WI69-RIPE
tech-c:         WH7765-RIPE
nic-hdl:        TRM1-RIPE
notify:         ripe-admin@terra.net.lb
mnt-by:         LB-TERRANET
changed:        ripe-admin@terra.net.lb 20020103
created:        2002-01-03T13:25:41Z
last-modified:  2006-11-29T08:37:34Z
source:         RIPE
```

Some of the domains used in the campaign were at some point registered to Lebanese addresses – a fact that was later changed by the operators.



	2014-12-05		2015-01-19
1	Domain Name:DOTNETEXPLORER.INFO	1	Domain Name:DOTNETEXPLORER.INFO
2	Domain ID: D47996051-LRMS	2	Domain ID: D47996051-LRMS
3	Creation Date: 2012-10-05T13:37:48Z	3	Creation Date: 2012-10-05T13:37:48Z
4	Updated Date: 2014-10-09T09:56:55Z	4	Updated Date: 2014-12-22T12:39:51Z
5	Registry Expiry Date: 2015-10-05T13:37:48Z	5	Registry Expiry Date: 2015-10-05T13:37:48Z
6	Sponsoring Registrar:Cloud Group Limited (R212-LRMS)	6	Sponsoring Registrar:Cloud Group Limited (R212-LRMS)
7	Sponsoring Registrar IANA ID: 84	7	Sponsoring Registrar IANA ID: 84
8	WHOIS Server:	8	WHOIS Server:
9	Referral URL:	9	Referral URL:
10	Domain Status: clientTransferProhibited	10	Domain Status: clientTransferProhibited
11	Registrant ID:DI_24370494	11	Registrant ID:PP-SP-001
12	Registrant Name:carima oun	12	Registrant Name:Domain Admin
13	Registrant Organization:N/A	13	Registrant Organization:Privacy Protection Service INC d/b/a PrivacyProtect.org
14	Registrant Street: beirut beirut	14	Registrant Street: C/O ID#10760, PO Box 16
15	Registrant City:beirut	15	Registrant Street: Note - Visit PrivacyProtect.org to contact the domain owner/operator
16	Registrant State/Province:beirut	16	Registrant City:Nobby Beach
17	Registrant Postal Code:961	17	Registrant State/Province:Queensland
18	Registrant Country:LB	18	Registrant Postal Code:QLD 4218
19	Registrant Phone:+961.961558668	19	Registrant Country:AU
		20	Registrant Phone:+45.36946676
20	Registrant Phone Ext:	21	Registrant Phone Ext:
21	Registrant Fax:	22	Registrant Fax:
22	Registrant Fax Ext:	23	Registrant Fax Ext:
23	Registrant Email:carima2010@live.com	24	Registrant Email:contact@privacyprotect.org
24	Admin ID:DI_24370494	25	Admin ID:PP-SP-001
25	Admin Name:carima oun	26	Admin Name:Domain Admin
26	Admin Organization:N/A	27	Admin Organization:Privacy Protection Service INC d/b/a PrivacyProtect.org
27	Admin Street: beirut beirut	28	Admin Street: C/O ID#10760, PO Box 16
28	Admin City:beirut	29	Admin Street: Note - Visit PrivacyProtect.org to contact the domain owner/operator
29	Admin State/Province:beirut	30	Admin City:Nobby Beach

A few words on the attackers' modus operandi

Disclaimer: Any assumptions made or conclusions drawn are based solely on our analysis of data from a limited group of targeted systems. As our sample size is admittedly restricted, it is possible that the attackers may also exhibit other behaviors that we have not encountered to date.

In the cases in which we have analyzed victim data, we saw the following interesting information:

One site to rule them all

Looking at victim data from the hosting companies, we noticed that the compromise of a single website led to the compromise of almost all the sites hosted by this service.

One is enough

Previously, we described that a typical attack begins with a vulnerability scan followed by a web shell injection to the compromised site. Based on analyzed victim data, we found that only one of the compromised sites per hosting service contained a web shell. The rest of the sites were most likely accessed using stolen admin credentials.

Continuous deployment

When we reviewed the logs of different victims, we found that version upgrades were almost always automated and occurred within seconds of each other.

OP-SEC? NOP-SEC!

In such a highly targeted operation, you would expect the operators to try and cover their tracks as much as possible. However, they left hints about their identity at almost every step of the way (see our earlier case for attribution). In the midst of our investigation of the infected machines, we discovered old tools or old key logging data collected by the malware was not removed, thereby exposing the operation to greater possibilities of discovery.

Hide in plain "site"

Dealing with an operation of this scope, with such carefully chosen targets, we would have expected a higher quality of malware development. These days, even the simplest malwares are packed to avoid detection, do not contain useless functions and code, or use obfuscated strings – all things we have noted to be poorly executed in *Explosive* and the other tools used in this campaign.

Appendix – Indicators

Explosive Hashes:

a00cd6d4d40cd0634c2d301f023b49c477bf9324640c8346a8596f4fceddd5aa

af5490785da0a859c5046791cf28fa5ad617122c21a99687db66356d1f8aefef

22d9e9193a341a617b30f3f9e50634dee0a03760badbeddf5cb34dda85192816

ad7422d6ffa43d4eea1b27d6a4842e69968bd1dde1c741afeba8a3271f9c5656

b74bd5660baf67038353136978ed16dbc7d105c60c121cf64c61d8f3d31de32c

08c0f0e6dadfc8f6a824e20d9de7fdd3e17f8ea115094379833c23834bbf9e79

a177b3a3add8acea3150de93be9f876c4ad8ba606bac5f88f20d682d2a89df57

37f4e9d0153221d9a236f299151c9f6911a6f78fff54c91b94ea64d1f3a8872b

d0f059ba21f06021579835a55220d1e822d1233f95879ea6f7cb9d301408c821 cc83382c823c15abd96cc3fd518f672ac0a6757142aac91a40dcdf1311f27ef9

a98099541168c7f36b107e24e9c80c9125fefb787ae720799b03bb4425aba1a9

e5b68ab68b12c3eaff612ada09eb2d4c403f923cdec8a5c8fe253c6773208baf

0008065861f5b09195e51add72dacd3c4bbce6444711320ad349c7dab5bb97fb

ea335556fecaf983f6f26b9788b286fbf5bd85ff403bb4a1db604496d011be29

bed0bec3d123e7611dc3d722813eeb197a2b8048396cef4414f29f24af3a29c4

b275c8978d18832bd3da9975d0f43cbc90e09a99718f4efaf1be7b43db46cf95

41dd95533d85a0fd099ee79fbb4c8699ae6f9299b74034b8bafa3b0ea4a1fb3a

97ab07c8020aead6ce0d9196e03d3917045e65e8c65e52a16ec6ef660dd96968

bd039bb73f297062ab65f695dd6defafd146f6f233c451e5ac967a720b41fc14

30196c83a1f857d36fde160d55bd4e5b5d50fbb082bd846db295cbe0f9d35cfb

52cb02da0462fdd08d537b2c949e2e252f7a7a88354d596e9f5c9f1498d1c68f

bc12d7052e6cfce8f16625ca8b88803cd4e58356eb32fe62667336d4dee708a3

fc085d9be18f3d8d7ca68fbe1d9e29abbe53e7582453f61a9cd65da06961f751

5d491ea5705e90c817cf0f5211c9edbcd5291fe8bd4cc69cdb58e8d0e6b6d1fe

d8fdcdaad652c19f4f4676cd2f89ae834dbc19e2759a206044b18601875f2726

50414f60d7e24d25f9ebb68f99d67a46e8b12458474ac503b6e0d0562075a985

3bedb4bdb17718fda1edd1a8fa4289dc61fdda598474b5648414e4565e88ecd5

1b76fdbd4cd92c7349bc99291137637614f4fb9598ae29df0a39a422611b86f8

ba168c69866ba2e370c9bfbfe06d5863af0e4b387ce05084928710af3c7c43ce

b74bd5660baf67038353136978ed16dbc7d105c60c121cf64c61d8f3d31de32c

03641e5632673615f23b2a8325d7355c4499a40f47b6ae094606a73c56e24ad0

ef47aaf4e964e1e1b7787c480e60a744550de847618510d2bf54bbc5bda57470

1952fa94b582e9af9dca596b5e51c585a78b8b1610639e3b878bbfa365e8e908

dea53e331d3b9f21354147f60902f6e132f06183ed2f4a28e67816f9cb140a90

973fbccbc6d917883d502c88cb7fadfc1a5657adbec377c7a4ed77292ebaeda9

5a310669920099cd51f82bc9eb5459e9889b6357a21f7ce95ac961e053c79acb

37f4e9d0153221d9a236f299151c9f6911a6f78fff54c91b94ea64d1f3a8872b

d0f059ba21f06021579835a55220d1e822d1233f95879ea6f7cb9d301408c821

5663b2d4a4aec55d5d6fb507e3fdcb92ffc978d411de68b084c37f86af6d2e19

388f5bc2f088769b361dfe8a45f0d5237c4580b287612422a03babe6994339ff

bdef2ddcd8d4d66a42c9cbafd5cf7d86c4c0e3ed8c45cc734742c5da2fb573f7

bfc63b30624332f4fc2e510f95b69d18dd0241eb0d2fcd33ed2e81b7275ab488

07529fae9e74be81fd302d022603d9f0796b4b9120b0d6131f75d41b979bbca5

d30f306d4d866a07372b94f7657a7a2b0500137fe7ef51678d0ef4249895c2c5

6674ffe375f8ab54cfa2a276e4a39b414cf327e0b00733c215749e8a94385c63

e2e6ed82703de21eb4c5885730ba3db42f3ddda8b94beb2ee0c3af61bc435747

f46ca3838f1843961a95274afc403300ba8c9cc7562f9fc1316f88f9453d3ec7

e463fdd4f769ea2d12cbe5a362edfba75fb251fe1b69c7437514a0f9863ee998

88cac72f0c754cca4f110e518476722497cb49465e69b10a030cd3f1b1b969c0

3becda7d601cf482d7ef236da6342239684694ed141a911601f321616440f6fa

35dcb7e62bac287e4e3f1fdcefdbf71e5dfe539208c36537ca1bbdce6749e612

f5c68a3ee7cc9ef8126687f035f9e46cdb90f03b4d3e10aaee38ad0793ee661a

a177b3a3add8acea3150de93be9f876c4ad8ba606bac5f88f20d682d2a89df57

47f45532108686fa535dbc32b5356f2005dc13c90f399170fa880ebd530f4645

af5490785da0a859c5046791cf28fa5ad617122c21a99687db66356d1f8aefef

487d8841582cb01231379fbffd7df87d4253c5dd3c26b06756490000d1ee1e82

ad7422d6ffa43d4eea1b27d6a4842e69968bd1dde1c741afeba8a3271f9c5656

08c0f0e6dadfc8f6a824e20d9de7fdd3e17f8ea115094379833c23834bbf9e79

Web shell hashes

5953c9bf800c67b67f1a3d9691119488d3a1d6e6c6691f8a15d28436cd7122a7

d7cb6fc59d81e935764653f99dd2cbf38aff7b1bf2a423e3846dcb17c52d871e

493007afc73a3d6573b2b53457d6c82e24e16591807565d6caf3e5b6b5d407a2

e33118afd512762c79d840b782dd5cfa2472c97613103e60f8d5427a0a26beb3

b64d6e0e09b6daab209d14f2e684d819433605763208fbfc901a9ab7fd62ce05

a616c039b0ffa2682f001a6978c5edfaac2c3f828b6b18de6bc91f4abaa2d9bb

c103c3c0a1d7983ca1951a72800346fad32a67b4be013a97361a3d85e0e8cd98

d1299a5c75882de2407f50b47c8a111349d4660e5b3fb7fdedfc4cfc2ef98a91

2f2e794064e28a4cd6eb0c0e10d929453367c4b01a55fadf15037817c55e9cdb

e584e0ae44a507d71cf97b490ea6a7ba9ce23b99f5c8bc6875ce60efa6bdf3df

4de07466f24a26311fe011f92c8b04e7c2c3ef4df8f5853bde523404ac06c34f

1dc13fe7f576f5c5ccac4230bdf2122d8351dd50266d0b712291ce59d1c788ae

709137152c150345578348529485afcfc711ba3cf1f55943f963809d3597adf7

Other tools hashes

22d9e9193a341a617b30f3f9e50634dee0a03760badbeddf5cb34dda85192816

26e64f95ee23a6ec3b9fb8f937bed8e6ea247379b1f0b2e95ef071dc113b420c

C&C servers

69[.]64[.]90[.]94

50[.]60[.]129[.]74

85[.]25[.]20[.]27

213[.]204[.]122[.]130

213[.]204[.]122[.]133

184[.]107[.]97[.]188

69[.]94[.]157[.]80

Static and Dynamic C&C updater servers

saveweb[.]wink[.]wk

carima2012[.]site90[.]com

explorerdotnt[.]info

dotnetexplorer[.]info

dotntexplorere[.]info

xploreredotnet[.]info

erdotntexplore[.]info

getadobeflashplayer[.]net