MMD-0009-2013 - RunForrestRun DGA "Comeback" with new obfuscation

Published: 2013-11-02 · Archived: 2026-04-05 18:18:17 UTC

```
domain:         YALKZSVUDYBEXFGD.RU
nserver:        dns1.webdrive.ru.
nserver:        dns2.webdrive.ru.
state:          REGISTERED, DELEGATED, UNVERIFIED
person:         Private Person
registrar:      REGGI-REG-RIPN
admin-contact: https:
created:        2013.04.15
paid-till:      2014.04.15
free-date:      2014.05.16
source:         TCI
Last updated on 2013.11.02 13:21:36 MSK
domain:         LOMXTGMGRSWLGRRN.RU
nserver:        dns1.webdrive.ru.
nserver:        dns2.webdrive.ru.
state:          REGISTERED, DELEGATED, UNVERIFIED
person:         Private Person
registrar:      REGGI-REG-RIPN
admin-contact: https:
created:        2013.04.15
paid-till:      2014.04.15
free-date:      2014.05.16
```

```
source:         TCI

Last updated on 2013.11.02 13:21:36 MSK

domain:         WZBDWENWSHFZGLWT.RU

nserver:        dns1.webdrive.ru.

nserver:        dns2.webdrive.ru.

state:          REGISTERED, DELEGATED, UNVERIFIED

person:         Private Person

registrar:      REGGI-REG-RIPN

admin-contact: https:

created:        2013.08.16

paid-till:      2014.08.16

free-date:      2014.09.16

source:         TCI

Last updated on 2013.11.02 13:21:36 MSK

domain:         JNFRQMEKHOEVPPVW.RU

nserver:        dns1.webdrive.ru.

nserver:        dns2.webdrive.ru.

state:          REGISTERED, DELEGATED, UNVERIFIED

person:         Private Person

registrar:      REGGI-REG-RIPN

admin-contact: https:

created:        2013.08.16

paid-till:      2014.08.16

free-date:      2014.09.16

source:         TCI

Last updated on 2013.11.02 13:26:32 MSK
```

```
domain:         VYGZHVFIUOMMKQFJ.RU
nserver:        dns1.webdrive.ru.
nserver:        dns2.webdrive.ru.
state:          REGISTERED, DELEGATED, UNVERIFIED
person:         Private Person
registrar:      REGGI-REG-RIPN
admin-contact: https:
created:        2013.08.16
paid-till:      2014.08.16
free-date:      2014.09.16
source:         TCI
Last updated on 2013.11.02 13:26:32 MSK
domain:         IMJOSXUHBCDONRCO.RU
nserver:        dns1.webdrive.ru.
nserver:        dns2.webdrive.ru.
state:          REGISTERED, DELEGATED, UNVERIFIED
person:         Private Person
registrar:      REGGI-REG-RIPN
admin-contact: https:
created:        2013.08.16
paid-till:      2014.08.16
free-date:      2014.09.16
source:         TCI
Last updated on 2013.11.02 13:26:32 MSK
domain:         BHIGMQCKBQHLEQLO.RU
nserver:        dns1.webdrive.ru.
```

```
nserver:       dns2.webdrive.ru.
state:         REGISTERED, DELEGATED, UNVERIFIED
person:        Private Person
registrar:     REGGI-REG-RIPN
admin-contact: https:
created:       2012.11.06
paid-till:     2013.11.06
free-date:     2013.12.07
source:        TCI
Last updated on 2013.11.02 13:31:37 MSK
domain:        NSJOSICXUHPIDHLP.RU
nserver:       dns1.webdrive.ru.
nserver:       dns2.webdrive.ru.
state:         REGISTERED, DELEGATED, UNVERIFIED
person:        Private Person
registrar:     REGGI-REG-RIPN
admin-contact: https:
created:       2012.11.06
paid-till:     2013.11.06
free-date:     2013.12.07
source:        TCI
Last updated on 2013.11.02 13:31:37 MSK
```
