An Inside Look at the Infrastructure Behind the Russian APT Gamaredon Group

Archived: 2026-04-05 15:41:41 UTC

Update May 24, 2022: Read our new blog post about Gamaredon group infrastructure, malware variants and infection tactics.

Recently, fellow researcher Vitali Kremez took a look at some new binaries from the Gamaredon Group. This is a Russian state-sponsored group that has been active since about 2013. The malware specifically is the Pteranodon implant, which provides a variety of functions such as remote command execution, downloading and executing other files, and collecting system data. It was the subject of a recent CERT UA blog post here (note: this site is in Ukrainian).

Of interest from Vitali's research was the callout to torrent-stel[.]space. This marks a change from their historical pattern of using dynamic DNS host names to registering their own domains. So, it was worth examining to what extent it is possible to map their current infrastructure. As of now, all the domains and IP addresses in this post are still resolving. (Though the specific URL returns permission denied if you try to interact)

Torrent-stel[.]space resolves to 185[.]248[.]100[.]121 which is also shared with splin-body[.]site and splin-body1[.]site. All three have been observed in similar infection chains and use spr_update.php as outbound web requests. The domains were registered in December 2018 and January 2019.

Of interesting note, one malware sample (hash: cbd0b2cb5c35a0c88494f10304213d494f3c220b6d5efb6c7cb8fb66f3267632) not only calls splin-body[.]site, it calls splin-upd[.]site which resolves to 195[.]88[.]208[.]196. That, in turn, gives us a few more domains of similar nomenclature (with similar malware infection chains) including one pivot from when they switched from dynamic DNS to their own domains in junk TLDs:

- torent-updates[.]ddns[[.]]net // this one is down probably because it was a typo, spies make mistakes too
- torrent-updates[.]ddns[.]net
- splin-upd[.]site
- splin-upd1[.]site
- torrent-supd[.]space
- www[.]torrent-supd.space

All except the typo domain are still up. Now, enough artifacts have been accumulated to find patterns of new domain registrations to find new domains as they are registered assuming they make no wholesale changes.

As an aside, we've been experimenting developing a machine learning classifier for domain names. Most of these efforts are whether domains are domain generation algorithms or not, this model uses resolution features of a domain to predict maliciousness. (As opposed to being benign or compromised) The model predicted these were malicious with a confidence of 88%.

ThreatSTOP Customers are automatically protected against the threat described in this blog.

Ready to try ThreatSTOP in your network? Want an expert-led demo to see how it works?
