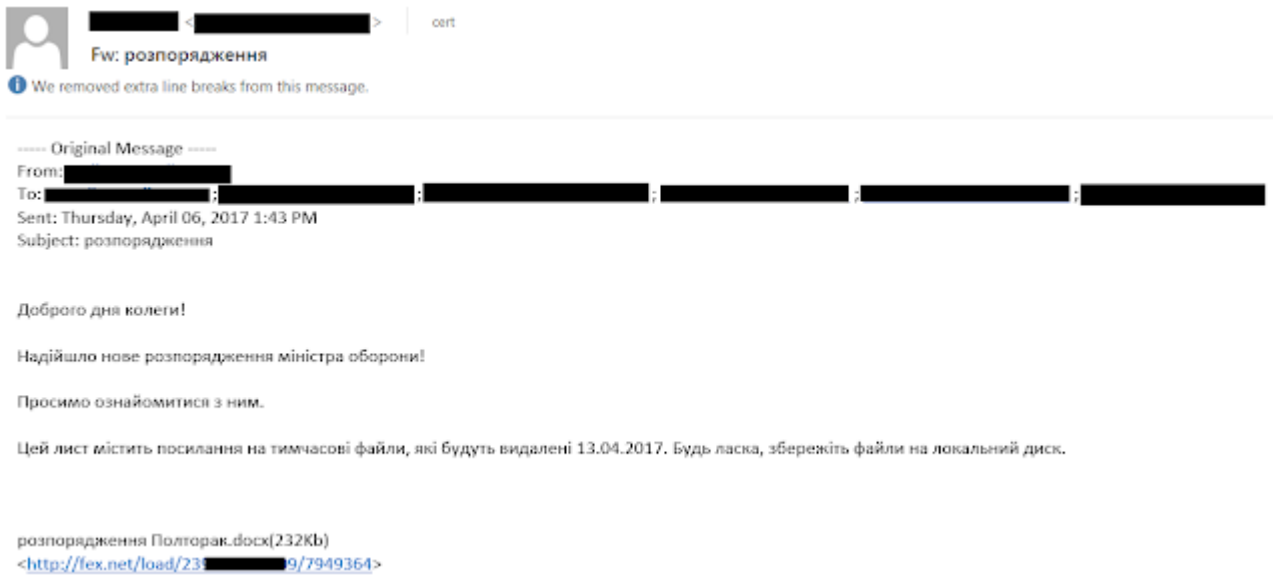


Targeted attack against the Ukrainian military

Archived: 2026-04-06 00:30:19 UTC

One more targeted attack against Ukraine that used spear phishing to deliver the DarkTrack backdoor through a fake prescription of the Minister of Defense of Ukraine. The target is CERT in the military domain.



The letter forces a receiver to download the prescription by the link until April 13, 2017.

The domain 'fex.net' in the link has been actively used to distribute malware:

3/64	2017-05-02 09:27:10	http://fs2.fex.net/load/173[redacted]7/8157923/Sofs2.fex.9495999/xfire_client_2.3.exe
3/64	2017-05-02 09:27:03	http://fs2.fex.net/load/239[redacted]9/7949364/%D1%80%D0%BE%D0%B7%D0%BF%D0%BE%D1%8C
3/64	2017-05-02 09:26:48	http://fs2.fex.net/get/8564[redacted]9959680/%D0%92%D0%BA%20%D0%B7%D0%B0%D1%80%D0%
3/65	2017-05-02 09:26:37	http://fs2.fex.net/load/173[redacted]7/8157923/Sofs2.fex.net/get/145631437712/7635168/KMSAuto.Li...
2/64	2017-05-02 09:26:08	http://fs2.fex.net/get/2735[redacted]7/9945234/discord_plugin_1.0.9.exe
2/64	2017-05-02 09:25:44	http://fs2.fex.net/get/4427[redacted]7/9120983/xfire_clientset7/fi/2008/182/6/1/inexperience_patch...
1/65	2017-05-02 09:25:06	http://fs2.fex.net/get/2735[redacted]7/9206862/razertalk_3.0login.exe
2/64	2017-05-02 09:24:26	http://fs2.fex.net/load/173[redacted]7/8157923/Sofs2.fex.net/get/145631437712/7635168/KMSAuto.Li...
6/65	2017-05-02 09:23:07	http://fs2.fex.net/load/783[redacted]3/10065547/41210412_dod.doc.exe
1/65	2017-05-02 09:21:43	https://fs2.fex.net/get/193[redacted]6/9495999/xfire_client_2.310.1.6%20Final.rar
1/64	2017-05-01 10:23:00	http://fs2.fex.net/load/239[redacted]9/7949364/%D1%80%D0%BE%D0%B7%D0%BF%D0%BE%D1%8C
5/65	2017-05-01 10:20:39	http://fs2.fex.net/load/239[redacted]9/7949364/%D1%80%D0%BE%D0%B7%D0%BF%D0%BE%EF%BF
1/64	2017-04-30 08:49:10	http://fs2.fex.net/load/173[redacted]7/8157923/Sofs2.fex.net/get/145631437712/7635168/KMSAuto.Li...
2/65	2017-04-30 08:47:43	http://fs2.fex.net/load/676[redacted]9/9008939/DiscordAcces:8089/gj1jk.exe

The downloaded file 'розпорядження Полторака.docx.exe' is an obfuscated .NET application (MD5: [01fb11b245a6a2525da77aebd2879dcf](https://www.md5hashgenerator.com/01fb11b245a6a2525da77aebd2879dcf/)). It copies itself as:

- c:\Documents and Settings\\Templates\winlogon.exe

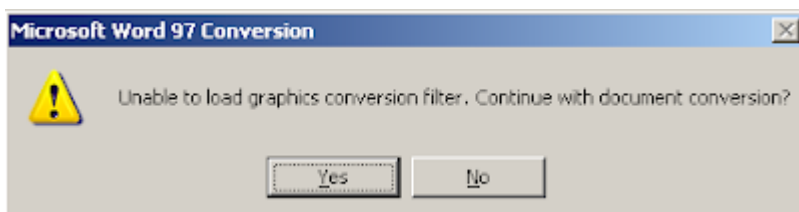
And drops the clean Word document:

- c:\Documents and Settings\\Local Settings\Temp\Docum.doc (MD5: b77f006667dd0a68de9c8ea30f2c80fe)

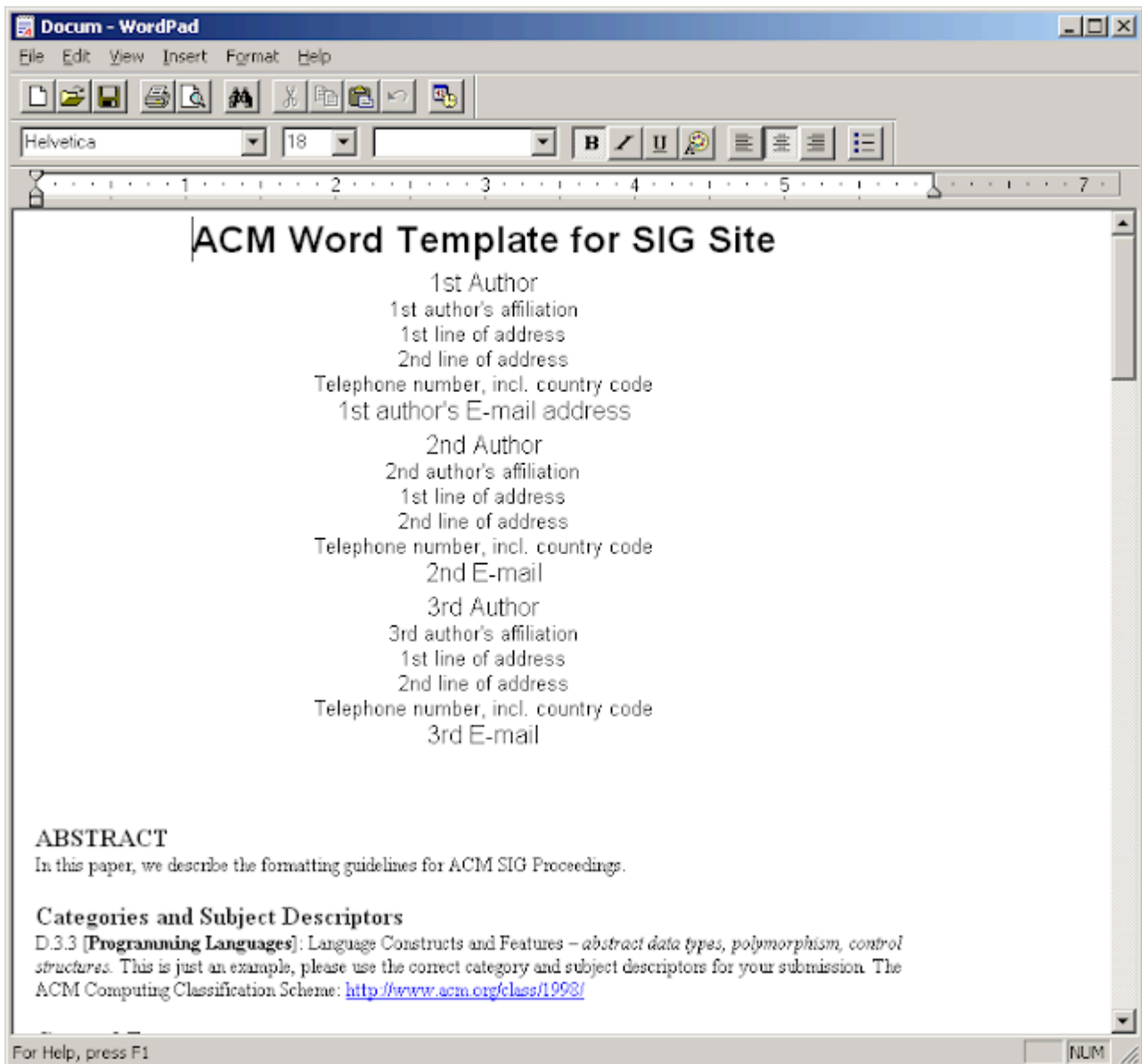
First, it executes 'C:\WINDOWS\system32\svchost.exe' and injects the Darktrack in the 'svchost.exe' process.

Then, it opens clean 'Docum.doc' to take a user's attention away.

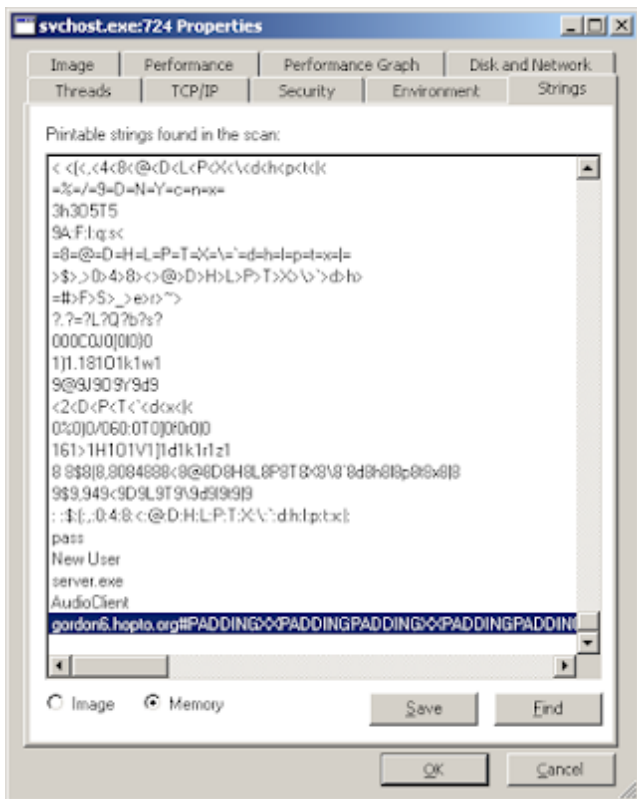
The following message is shown on execution:



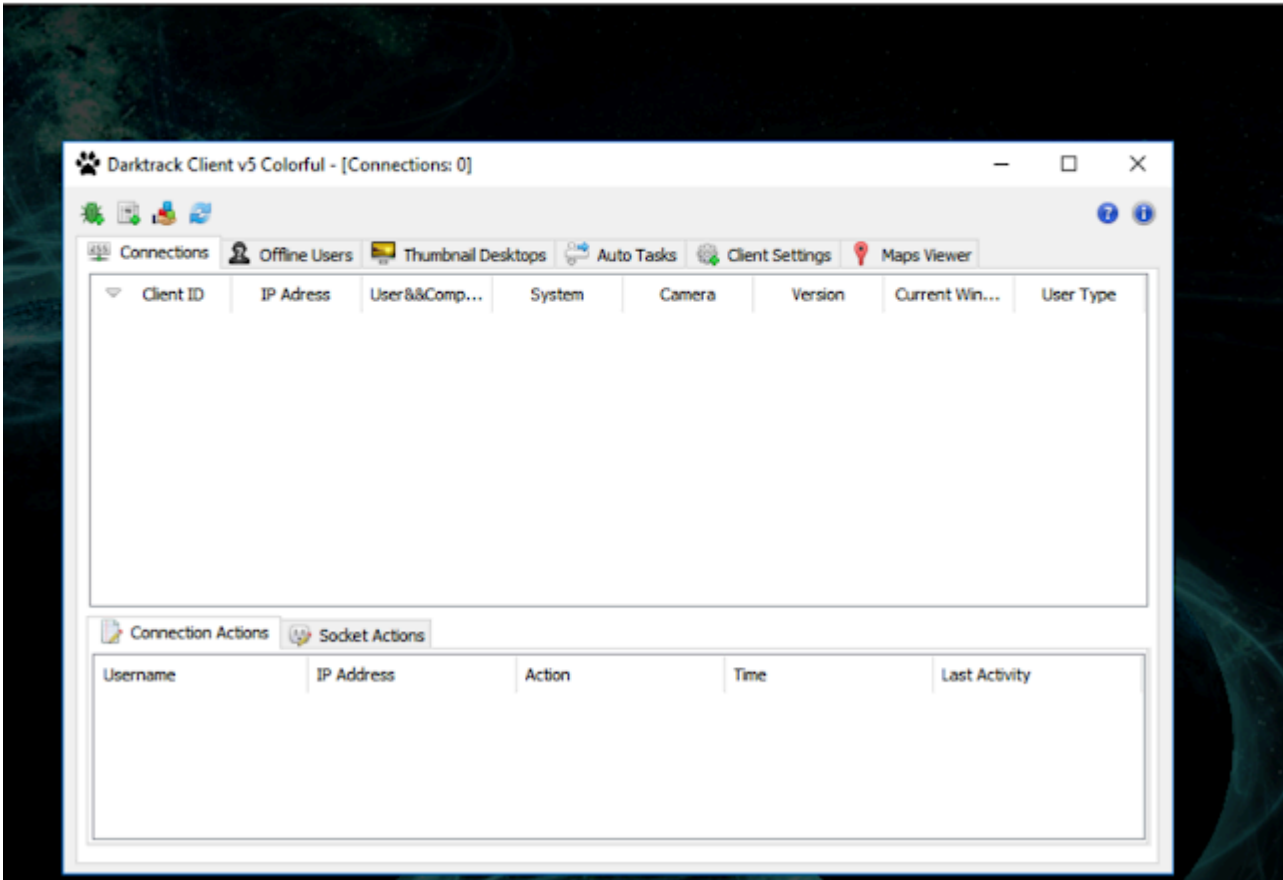
Then, it opens the embedded document:



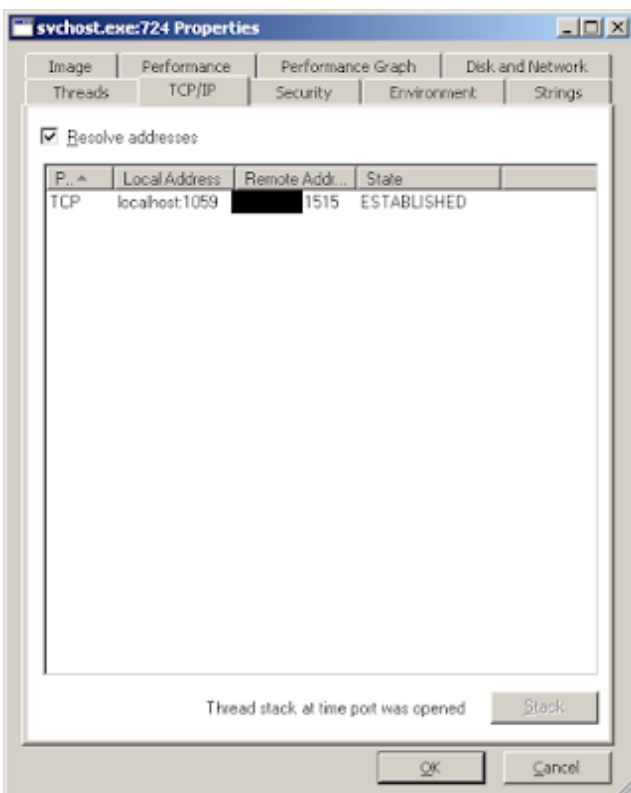
The malicious process injects the backdoor's code into the system 'svchost.exe':



The backdoor is the Darktrack remote administration tool.



The client connects to the C&C's 1515 port.



The Darktrack client uses the proxy service 'hopto.org' to connect to the attacker's C&C.

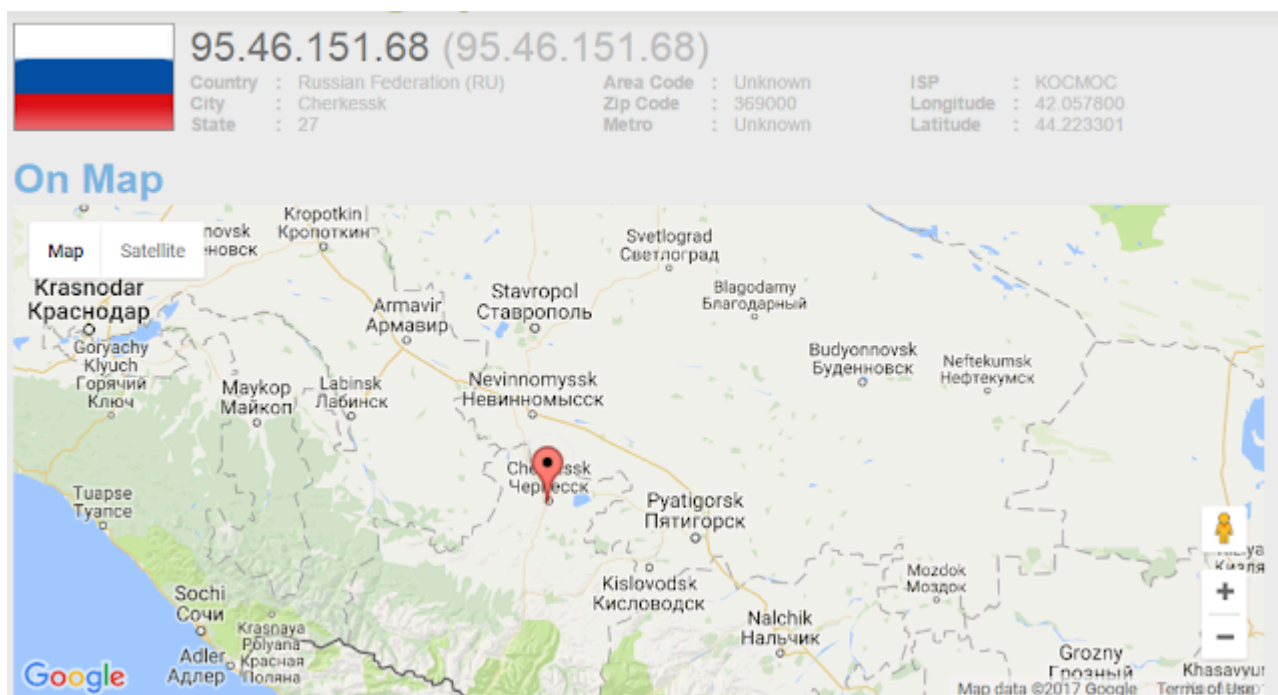
gordon6.hopto.org has been resolved to the following IPs:

95.46.151.68

62.76.106.236

92.38.37.15

All of the IPs are located at one place in Russia.



Network IoCs:

gordon6.hopto.org

fex.net

95.46.151.68

62.76.106.236

92.38.37.15

Source: <https://nioguard.blogspot.de/2017/05/targeted-attack-against-ukrainian.html>