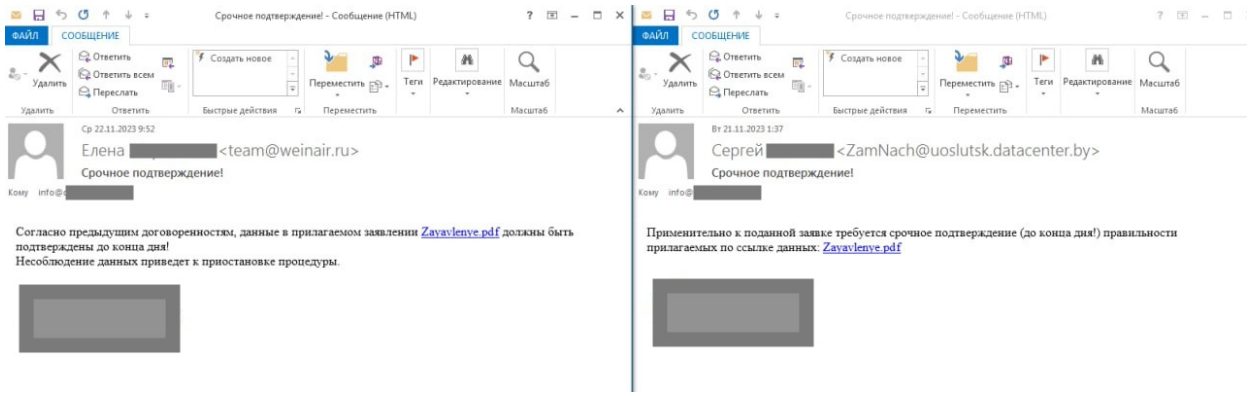
Кибершпионы из XDSpy атакуют российских металлургов и предприятия ВПК

EditorF_A_C_C_T ⋮⋮ 11/23/2023

EditorF_A_C_C_T 23 ноя 2023 в 13:24

Эксперты департамента Threat Intelligence (Киберразведка) и Центра кибербезопасности компании F.A.C.C.T. предупреждают о новых атаках кибершпионской группы **XDSpy**.

Вчера, 22 ноября, и позавчера, 21 ноября, были обнаружены вредоносные рассылки, нацеленные на почту одного из российских металлургических предприятий, а также НИИ, занимающийся разработкой и производством управляемого ракетного оружия.



В обоих случаях в подписи стоит логотип российского научно-исследовательского института, специализирующегося на проектировании объектов ядерного оружейного комплекса, а в качестве отправителя была указана электронная почта некой логистической компании из Калининграда.

Кроме того, было обнаружено еще одно письмо, отправленное российским металлургам, но уже с белорусского адреса.

Киллчейн этой ноябрьской кампании такой же, как и в описанных ранее нами летних атаках XDSpy — технические подробности мы приводили в этом блоге на Хабре.

Напомним, что большинство целей XDSpy находятся в России — это правительственные, военные, финансовые учреждения, а также энергетические, исследовательские и добывающие компании. Хак-группа активна с 2011 года, однако международные специалисты до сих пор не определились, в интересах какой страны она работает.

Индикаторы компрометации:

ZIP
Zayavlenye.zip

MD5: 9a4a3b0dc729714252421815197 74cd4
SHA-1: 719070fb1fc18b235c393b66d5a7cc8ab0a15661
SHA-256: e860e512ee7fef05e960b2c2d947463cf6ce5df3274733314bd55c6f80df76da

Zayavlenye.zip
MD5: d73d7f598e63a2c9a22ea5854c088b74
SHA-1: 731e143d2ee11ebd4716dae3185d33f0863d897f
SHA-256: 82cce34df5fa97314ea9307d13e2cc1a98f391b31dd75bb86f6653be4a5d29ac

LNK
Zayavlenye.lnk
MD5: d5598e32a3db5b79ed45110fb34c919f
SHA-1: ac2e52774fe7bc390188cf274566c096ea3f7b48
SHA-256: 02b274f864b4874e06d79f8726c51ecfc7fdf4abde8bd5cfcc576885bac77eae

Zayavlenye.lnk
MD5: 212aeb44a57b10670fb80e192d4763ad
SHA-1: 257aa503b833cc6f6957cce41deb0e13a32a0a00
SHA-256: f06acecc4470137bf1c9caa2dbe8e96ba01d8af0596b25e3cecb1b76822403d2

XDSpy.CSharpDownloader
.DS_Store
MD5: 03434f60597f1a83d07661519572c3b1
SHA-1: a6ecef07ff3a9691d585133a8c92bc8eca3e87ff
SHA-256: b0355a523d3145f63baab5e8a4fb7108ebaacead044e77af8a3fc999be1c59ac

.DS_Store
MD5: 6aabe65825d5223fc089a3ef40d743e6
SHA-1: 8aa6654b934af0aabaacebe824359080790063c0
SHA-256: 7847ef05e2a57ac702a56cfa4908c167ae32994a7870a6a6ee093d0086e42d29

XDSpy.Mainmodule
InternalDiagnosisCollector.exe
MD5: 9561a3b5c4b4d9413a6ad51efe48a3c0
SHA-1: d36369f17901b2379b96b95ffaacb0ef538990e8
SHA-256: 03f24aff78597c95cb3cc5324ee29f4e301e5c47340c60c2223a9d6e0edda131

InternalDiagnosisCollector.exe
MD5: e949b7f8b725fefd63788700f4ee2f68
SHA-1: 297a5590dc9ca89f4cf6cb9e308061fb2f98d0f2
SHA-256: f90e2ea780399d9bcc4ae2aa92fe271197ced5c6db4f88191fd0b3b271241cfd

URLs:
hxxps://downmyload[.]com/doc/Zayavlenye/Zayavlenye/indexer/dwnder/4ci0rfqvmx0q21cl67
hxxps://storagebox4you[.]com/doc/Zayavlenye/Zayavlenye/indexer/dwnder/7gundjrjs3fuevc9rj
hxxps://storagebox4you[.]com/doc/Zayavlenye/Zayavlenye/indexer/dwnder/hh4r9m6e3w89npmatt
hxxps://downmyload[.]com/doc/Zayavlenye/E/indexer/dwnder/4ci0rfqvmx0q21cl67

hxxps://storagebox4you[.]com/doc/Zayavlenye/E/indexer/dwnder/7gundjrjs3fuevc9rj
hxxps://storagebox4you[.]com/doc/Zayavlenye/E/indexer/dwnder/hh4r9m6e3w89npmat
hxxps://downmyload[.]com/doc/Zayavlenye.pdf
hxxps://storagebox4you[.]com/doc/Zayavlenye.pdf

C2:
enjoyever[.]com
coolpelear[.]com