

Перечни идентификаторов компрометации

II раздел, пункт № 6.

Индикаторы компрометации хакерской группировки Bloody Wolf	
Сетевые индикаторы	
kazsrv[.]online	salyk-notofocations[.]com
ozhet[.]com	1994collective13[.]com
yessenov[.]com	1994collective[.]com
hxxps[:]//kazsrv[.]online/dl/HTCTL32[.]DLL	hxxp[:]//salyk-notofocations[.]com/1/msvcr100[.]dll
hxxps[:]//kazsrv[.]online/dl/NSM[.]lic	hxxp[:]//salyk-notofocations[.]com/1/kbd101c[.]DLL
hxxps[:]//kazsrv[.]online/dl/run[.]bat	hxxp[:]//salyk-notofocations[.]com/1/qwave[.]dll
hxxps[:]//kazsrv[.]online/dl/advpack[.]dll	hxxp[:]//salyk-notofocations[.]com/1/pcicapi[.]dll
hxxps[:]//kazsrv[.]online/dl/AudioCapture[.]dll	hxxp[:]//salyk-notofocations[.]com/1/kbd106n[.]dll
hxxps[:]//kazsrv[.]online/dl/PCICL32[.]dll	hxxp[:]//salyk-notofocations[.]com/1/tcctl32[.]dll
hxxps[:]//kazsrv[.]online/dl/client32[.]exe	hxxp[:]//salyk-notofocations[.]com/1/AudioCapture[.]dll
hxxps[:]//kazsrv[.]online/dl/kbdibm02[.]DLL	hxxp[:]//salyk-notofocations[.]com/1/kbdlk41a[.]dll
hxxps[:]//yessenov[.]com/3neQSPnRI26Qt6ajZj36g2RmzGCA/opovesheniyeurlic/nalogovie narusheniya/1jRpSSmwm5im/client_secret/oauth2/ru/gosuslugi/36b425a1cad679275fa6b04e237f494bf25bc66c/ReshenieJCP[.]jar	hxxp[:]//salyk-notofocations[.]com/1/nskbfltr[.]inf
hxxps[:]//kazsrv[.]online/dl/nskbfltr[.]inf	hxxp[:]//salyk-notofocations[.]com/1/PCICHEK[.]DLL
hxxps[:]//kazsrv[.]online/dl/tcctl32[.]dll	hxxp[:]//salyk-notofocations[.]com/1/run[.]bat
hxxps[:]//kazsrv[.]online/dl/kbd106n[.]dll	hxxps[:]//salyk-notofocations[.]com/rassylkazadolnikam/opovesheniya-o-narusheniyah-zadekabr/recourses-java-updater/direct-egov-kz-december/00af59a82188eff7/NCALayerUpdatedRU[.]jar

hxxps[:]//ozhet[.]com/russian-federation/36b425a1cad679275fa6b04e237f494bf25bc66c/gosuslugi/ru/oauth2/client_secret/1jRpSSmwm5im/nalogovienarusheniya/opovesheniyurlic/3neQSPnRI26Qt6ajZj36g2RmzGCA/CryptoProJCP[.]jar	hxxps[:]//salyk-notofocations[.]com/rassylkazadoljnikam/opovesheniya-o-narusheniyah-zadekabr/recourses-java-updater/direct-egov-kz-december/00af59a82188eff7/NCALayerUpdatedKZ[.]jar
hxxps[:]//kazsrv[.]online/dl/kbdlk41a[.]dll	hxxp[:]//salyk-notofocations[.]com/1/NSM[.]lic
hxxps[:]//kazsrv[.]online/dl/msvcr100[.]dll	hxxp[:]//salyk-notofocations[.]com/1/remcmdstub[.]exe
hxxps[:]//kazsrv[.]online/dl/remcmdstub[.]exe	hxxp[:]//salyk-notofocations[.]com/1/update[.]bat
hxxps[:]//kazsrv[.]online/dl/PCICHEK[.]DLL	hxxp[:]//salyk-notofocations[.]com/1/PCICL32[.]dll
hxxps[:]//kazsrv[.]online/dl/client32[.]ini	hxxp[:]//salyk-notofocations[.]com/1/kbdibm02[.]DLL
hxxps[:]//kazsrv[.]online/dl/ir50_qcx[.]dll	hxxp[:]//salyk-notofocations[.]com/1/ir50_qcx[.]dll
hxxps[:]//kazsrv[.]online/dl/qwave[.]dll	hxxp[:]//salyk-notofocations[.]com/1/client32[.]exe
hxxps[:]//pastebin[.]com/raw/hLUWEXTH	hxxp[:]//salyk-notofocations[.]com/1/ir50_32[.]dll
hxxps[:]//kazsrv[.]online/dl/update[.]bat	hxxp[:]//salyk-notofocations[.]com/1/HTCTL32[.]DLL
hxxps[:]//kazsrv[.]online/dl/pcicapi[.]dll	hxxp[:]//salyk-notofocations[.]com/1/client32[.]ini
hxxps[:]//kazsrv[.]online/dl/KBDSF[.]DLL	hxxps[:]//pastebin[.]com/raw/pruy96p1
hxxps[:]//kazsrv[.]online/dl/ir50_32[.]dll	hxxp[:]//salyk-notofocations[.]com/1/advpack[.]dll
hxxps[:]//kazsrv[.]online/dl/kbd101c[.]DLL	hxxp[:]//salyk-notofocations[.]com/1/KBDSF[.]DLL
Хэш-суммы файловых индикаторов компрометации (sha256)	
6ae7b754e74a6aa9f803037a8252cf5acfe5b8e8d82ae4b9b9a38826c4586702	
7438790a29940e20e503ef3987769e3a722e832d2bffa7b608162c0bd52c9e5c	
cc02f7a3906b84946e6f43f942b03d07c9f0d2ff9991e7c8f08845635ffca305	
9ec2ef504d28ba240f47f2e520c89604596b97c5045cff61a6735709bb8369c2	
0ee9f6312c4db254649e475395b071c48588693ced205fac5ecdc73d1c249ef5	

8f527a9a856daea8eac6229d86b46cf767ffbb1554e98073a8ddcc1b8e00ec9a
abd12f775d030d170fe4868dbbfff37b34f1decfa3023c2bd095f0affdd7d5cde
db9e7e615feea78fb1da1d063c5880c5069622641f96fd153b4bf347901bbcbf
482c35593241a180e066bcb5871628306aacff29f5cdb8989809456d3c7d2c00
745cb4422aaeffd070e167dfec46c6b44b2e155f96c0ac60ca645985e62c2ab4
8f23e6c903fef918a1f45ec0864f5826f503f5d07c910ba8751266a17126f77b
b41aa120d4b8de188344a80d0e8330d31248ddc635e3f660572eb2b4417a1a1e
be556bc2c58e56e6054ec017df771cf086cb6e4bfeafa5e6f2da5e6068ee1262
6e2ed736880f1eb96579d0306f463b59f34099018657d59c466064aefb5a817d
e4a6bbf0e2e66d660a2b5c01ecea8e22551e9edba114bf43b62b63133fadb21c
51a53f5323607c1af14d002409f19f19f802be38ebe8389dc88b7c0ed370942d
52826068ad2b9175dbb619019984c9b185cc0d5dc96c58698c0a32e9f64cc98a
f40835024db1f4b148d739b78243e0055888cad4028927d3127e1d85fdf4c9d4
b2c776a9554e2919f7a7e287f2954674fc5dbd6a10f342558ad98b606d664075
f7da65498b26ae9245ecb3133bcc34122655a759db333914d2969761956810d5
473596b2f09910b0484bac76190de4868b7d4ac756c46c102dc3bd91609d239e
062f8562115d81c435c9024de6bf64f49ffa918fb06fc06b770119dfc720d416
cf661780280b4962d04cf9970db3877f9f7316fcb1dc503365474fc2e10871e8
ca93f4b1eea0ddbffd8f217bbde9f14d04f7b0b5a6c396af65dfecfb267976d
07b06c09127c23fd9a983793ec7886cd2ea17a3d5ccc5b74133530ab1903686f
3ff5d7da088da36d79f295091568dc1a39796a1b70f91aafbbaa1ba5ae62597eb
85f5b09c7bea94809552755e6b3acde58c1d6ca1f9dcb78bc0921a08152e5322
10cd57a425b72d4f21c8f88b5d4033fad4477dd147cdf13b013f6391168c63bb
bb2b848ea3c6467e924b8c5717fa511714b79e27fc0ab28a1001aa09cc277c8a
c493e0223f1d490e647f0103b0eb4ed546624e98f6a3d0de2ec9debcbab3e5f0
dd6b56dd9be9f37c0c4394dc26290cad3113a9a47e94c06e5ece5ea67adb9667
23798a5c9ac923213a636b7fdbc5b0a40a32c79bb0b4750e030e7cbcca55c35

II раздел, пункт № 13.

Индикаторы компрометации	
Сетевые индикаторы	
45[.]93[.]95[.]105	hxxps[:]//telegra[.]ph/1610677127648-01-30-2

45[.]93[.]94[.]195	hxxps[:]//telegra[.]ph/1610677127648-01-30-3
45[.]83[.]40[.]225	hxxps[:]//telegra[.]ph/974263505263-01-29
45[.]60[.]167[.]209	hxxps[:]//telegra[.]ph/974263505263-01-29-2
45[.]223[.]230[.]112	hxxps[:]//telegra[.]ph/974263505263-01-29-3
212[.]80[.]205[.]31	hxxps[:]//telegra[.]ph/974263505263-01-29-4
185[.]229[.]226[.]223	hxxps[:]//telegra[.]ph/337849882878-01-28
212[.]80[.]206[.]103	hxxps[:]//telegra[.]ph/1065022638108-01-26-2
188[.]191[.]147[.]222	hxxps[:]//telegra[.]ph/1065022638108-01-26-3
212[.]80[.]206[.]210	hxxps[:]//telegra[.]ph/428609015723-01-25
83[.]229[.]70[.]231	hxxps[:]//telegra[.]ph/1792195393338-01-24-2
hxxps[:]//telegra[.]ph/973163812793-02-06	hxxps[:]//telegra[.]ph/519368148568-01-22
hxxps[:]//telegra[.]ph/336750190408-02-05	hxxps[:]//telegra[.]ph/610127281413-01-19
hxxps[:]//telegra[.]ph/336750190408-02-05-2	hxxps[:]//telegra[.]ph/700886414258-01-16
hxxps[:]//telegra[.]ph/336750190408-02-05-3	hxxps[:]//telegra[.]ph/64472791873-01-15
hxxps[:]//telegra[.]ph/1700336568023-02-04-2	hxxps[:]//telegra[.]ph/791645547103-01-13
hxxps[:]//telegra[.]ph/1063922945638-02-03-2	hxxps[:]//telegra[.]ph/155231924718-01-12
hxxps[:]//telegra[.]ph/1063922945638-02-03-3	hxxps[:]//telegra[.]ph/882404679948-01-10
hxxps[:]//telegra[.]ph/1063922945638-02-03-4	hxxps[:]//telegra[.]ph/245991057563-01-09
hxxps[:]//telegra[.]ph/427509323253-02-02	hxxps[:]//telegra[.]ph/973163812793-01-07
hxxps[:]//telegra[.]ph/427509323253-02-02-2	hxxps[:]//telegra[.]ph/336750190408-01-06
hxxps[:]//telegra[.]ph/427509323253-02-02-3	hxxps[:]//telegra[.]ph/427509323253-01-03
hxxps[:]//telegra[.]ph/427509323253-02-02-4	hxxps[:]//telegra[.]ph/611226973883-12-31
hxxps[:]//telegra[.]ph/1791095700868-02-01-2	hxxps[:]//telegra[.]ph/65572484343-12-27
hxxps[:]//telegra[.]ph/247090750033-01-31	hxxps[:]//telegra[.]ph/1429158861958-12-26-2
hxxps[:]//telegra[.]ph/247090750033-01-31-2	hxxps[:]//telegra[.]ph/792745239573-12-25
hxxps[:]//telegra[.]ph/247090750033-01-31-3	hxxps[:]//telegra[.]ph/156331617188-12-24
hxxps[:]//telegra[.]ph/247090750033-01-31-4	

II раздел, пункт № 14.

Сетевые индикаторы компрометации группировки ТА558	
139[.]144[.]212[.]135	paste[.]jee/d/4Pr]ryGx/0
172[.]232[.]4[.]203	paste[.]jee/d/1YNomP2m/0
45[.]79[.]137[.]187	paste[.]jee/d/Z4qloC5]

172[.]235[.]133[.]243	paste[.]ee/d/wcr6kvXw/0
172[.]233[.]129[.]114	paste[.]ee/d/TK74WUB4/0
172[.]232[.]170[.]236	paste[.]ee/d/9c9jQeiE/0
172[.]232[.]163[.]207	paste[.]ee/d/spi57
45[.]74[.]19[.]84	paste[.]ee/d/0aXad
70[.]34[.]197[.]128	tau[.]id/ze87s
172[.]234[.]217[.]97	paste[.]ee/d/5nJBg
45[.]56[.]102[.]63	paste[.]ee/d/62kvY
172[.]232[.]172[.]53	tau[.]id/c9izr
172[.]232[.]189[.]152	tau[.]id/34x8c
172[.]232[.]172[.]123	paste[.]ee/d/Pz2XE
172[.]232[.]189[.]7	ye[.]pe/0y2k
75[.]102[.]51[.]237	paste[.]ee/d/VkPF6
baltictransline[.]store	paste[.]ee/d/wsePT
automaxtool[.]me	paste[.]ee/d/S8WBj
akcalogistics[.]shop	paste[.]ee/d/tggWc
naft-dz[.]shop	paste[.]ee/d/7tUhO
vervo[.]lat	tau[.]id/y3kre
laceys[.]icu	paste[.]ee/d/Noi6G
maximum[.]icu	tt[.]vg/IsjCX
biatr[.]ooguy[.]com	paste[.]ee/d/oDnyo
abspedition[.]icu	tt[.]vg/PqPsi
midae[.]com	l-to[.]com/ru7285wa
executivesship[.]com	shtu[.]be/e79171
tau[.]id/0vzd8	en0[.]de/serverrrrr
pluse-tr[.]com	qr-in[.]com/HDYwZbx
hdvysy[.]com	isols[.]co/zXTgU
wallpapercave[.]com/uwp	bot[.]ax/hNZdz