هشدار مرکز ماهر در خصوص نوع جدیدی از باج افزار ایرانی-روسی با نام زئوس

باج افزار اندرویدی جدیدی که گونه‌ای از باج افزار زئوس به حساب می‌آید درحال گسترش با سرعت بالایی در پیام‌رسان تلگرام و وب سایت‌ها می باشد. تاکنون نسخه اولیه این بدافزار منتشر شده است که در آن عبارت رمز درخواستی در کد قرار گرفته است و می‌توان آن را با تحلیل کد به دست آورد. عدم وجود نظارت درست روی کانال‌ها و برنامه‌های منتشر شده در تلگرام باعث به وجود آمدن بازارهای سیاهی شده است که بدافزارهای مختلف از هکرهای روسی خریداری شده و با کمی تغییر در شکل آن و ترجمه برخی عبارات به فارسی به طور عمومی تحت عناوینی فریبنده منتشر می‌شوند.

نحوه انتشاربرنامه مخرب:

براساس تحقیقات انجام شده، کانال‌ها و گروه‌هایی ایجاد شده است که در آن‌ها بدافزارها به فروش می‌رسند. رایج‌ترین این برنامه‌ها، بدافزارهای روسی هستند که کد آن‌ها به افراد مختلف فروخته می‌شود و آن‌ها نیز با داشتن اندک دانش برنامه‌نویسی قادرند برنامه را تغییر داده و به‌صورت بدافزار ایرانی، تحت عناوین مختلفی از کاربران سوءاستفاده کنند. بررسی‌های مرکز ماهر نشان می‌دهد باج افزار موردنظر نیز، که خود را نوعی از باج افزار زئوس معرفی کرده، در کانال‌های تلگرامی در حال فعالیت می-باشد. یک نمونه از برنامه مخرب مربوط به این باج افزار که در شکل ۱ ، تحت عنوان برنامه‌ایرانسل توزیع شده است.

شکل ۱

لیست برنامه‌های دارای باج افزار زئوس

در لیست زیر برخی از نمونه‌های یافت شده از باج افزار آورده شده است. بدیهی است کاربران محترم با دیدن این عناوین در کانالهای تلگرام و وب سایت های موجود از دانلود و نصب این برنامه ها اکیدا خودداری فرمایند.

نام برنامه	نام بسته	مقدار MD5	لینک تحلیل	سایز
[Z]{eus}©[b]{undle}	Zeus.bundle.com	c33611536443d0dbcbd4e9c5a667a468	https://koodous.com/apks/2b9426d54b8a6f585a315eed3ee0f0d9ca7fa3bd70714bc4d986b3bb36af3ddb	292.5 kB
[Z]{eus}©[b]{undle}	Zeus.bundle.com	0f5bbe7d47c2198d4f286f4e41cf1baa	https://koodous.com/apks/f58bceb580898ee709c3f188064a1dd802ac60e66779973b5f666ccc6e20ce4a	292.5 kB
My Irancell – VIP	Myirancell.VIP	4ccf5610bfb8a0a30d162f3d39f22228	https://koodous.com/apks/437bbf5a5dcd0cd4f2e617b51d67eee1d5fc3bc28fe93f558da7ef2f0660694f	5.3 MB
My Irancell – VIP	Myirancell.VIP	e883c5961bf9eb4e8ef9518dd89ea13e	https://koodous.com/apks/0b89a6a48c3a9d2cb6999b7cb606b78a9cc91637ade147cffbae01bd7c72982b	33.8 kB
Coin Up	Myirancell.VIP	cd5262fb6fa52aee76f27439f6fcbb6c	https://koodous.com/apks/db2da4dc015a2817d00f23da5e22ca8da1f6414d06cadfee959e1ca4e727d5c5	61.4 kB
تلفن فوتبالیست‌های معروف	com.lololo	5855410be6eccdc59d557c10cb51438d	https://koodous.com/apks/21af3bf4082d874cfb1b20ee3f5e0555583d54631a23c0841a56366826bc9585	194.7 kB
hack telegram	com.lololo	dbb0a28e2de74e0cd30671c85f35e05d	https://koodous.com/apks/e44ba21b07f85c5ccc540e84d691eb99cb84d0e3932188443c29653c1d537621	192.0 kB
آموزش هک چنل	com.lololo	d3db211e492698195a14d7a1d7d6fe0b	https://koodous.com/apks/75b982d839a37587e552361fa23daba8d5bbd8708c07320f3b84a1b1fb630cfc	187.4 kB
تلفن فوتبالیست‌های معروف	com.lololo	069772b42e893ed2f06e8de397a2ee8e	https://koodous.com/apks/be2338a0808b187f6452c0c1cb1241ddc98deafb5312590760bdf44fd765c4ae	194.6 kB

ساخت کد شارژ	com.lololo	61d5be46121a35965b379c1c27b7ecf8	https://koodous.com/apks/ff6045a8e41795ff24755f4178cede92941db0f66992426569b613bc94329051	187.3 kB
صیغه یاب	com.lololo	944d82696a0365733fe41c8abf49bbcf	https://koodous.com/apks/8b8a91d6900d26ace9781d8399e9e11417960bc69336ce6b76cca6d66526a736	11.3 MB
تلفن فوتبالیست‌های معروف ایرانی	com.lololo	a02935fd346527d96dd4d498b30d19e5	https://koodous.com/apks/086a6a49f2410abc1ad99c6616634b26e65167605c7d3e26463e7eed4e2c4720	190.6 kB
پروفایل چکر	com.lololo	dcc428033fb26d97e8bc3808a93c61ec	https://koodous.com/apks/874933efd403565dc9d09a00ee42c33a92e51c1b1bb605ed863f8a8dbae21b62	193.7 kB
هک فالور	com.lololo	b39acca5b898f3c4aa8a5c7773f3a049	https://koodous.com/apks/5397b483d77561993a956bca71bbb9c134c4f88ee760cb34f9b5fd5ee841f54f	195.6 kB
موبوگرام۲(روح)	com.lololo.hacker	e3e66ad7d1f1bad8cfcd69e2dbb23e69	https://koodous.com/apks/fe1c2b15e63ad06ad6e4286c859f2519ab9141f5bd30cac2d1c814b4bbefb85b	12.8 MB
آنتی ریپورت	com.lololo	0d51baa143c8568a7f373bcfe9c96037	https://koodous.com/apks/c5427ba018e952aeeb4aa2f83d2669c01701bd01682edd4e6cfbe0c0c60ef81a	95.9 kB
فالور (بینهایت)	com.lololo	b9809ef78465c2522b3fb1ed8da5d554	https://koodous.com/apks/5afce9c25616628d879c692201c4595d9ed567193a250c779a58155362fb4394	189.1 kB
آموزش هـک	com.lololo	fa09ade5dddffc0974aacab8b2ed062c	https://koodous.com/apks/9c1f614d8edd7a134d715010feca11e5e2541373f96ecff0b30a55a62c610ae2	199.2 kB
سین ساز	com.lololo	845379f1944be32c31d54d7112863d1f	https://koodous.com/apks/a398a1061b9eab3c61c3c82dd8975f427aae2bef9bf516445cc521584d7a0244	195.8 kB
فالوئر گرام مود شده	com.lololo	c8fcc1bb750965e6b0919172f00c3fbc	https://koodous.com/apks/c68d6ea481e25e8e9806392719468e933ddba814c5b3a7dbfa3f06c8a736889d	186.5 kB
Mobogram	com.lololo	390348878ef3cac90e815aa3b812f9f0	https://koodous.com/apks/49fc74de95a9f31783be6de60c7a25f9e141	194.9 kB

	963495c320a734c9c8558def4345			
195.0 kB	https://koodous.com/apks/0112fefa8b7b4c403b4a832b4ace65204a5a3173a7007d8348d8f12290dc40d1	037fd4d0270669a8be81ea0c33638ee1	com.lololo	هک شارژ
193.1 kB	https://koodous.com/apks/f3f9aad0be4f603545cebae50b452ed35f88da29387e752dfef36cd2e19017fc	6bbcbd1482b5b949934d8ffb0f130569	com.lololo	Hack Gmail
193.8 kB	https://koodous.com/apks/335a5f29d8932382d01f3a77b48c0a1f5eaaa14433eb4c3eec2cdeea343f63df	01bc86296ffe42eaccca7c7abc65b4ad	com.lololo	Game Hacker
201.3 kB	https://koodous.com/apks/e282724b3803a6faf81608f071dbe40e54a91b67f9ea54a0dd58784f5b669f70	681eabd1aeda87a41538b73b8028ea93	com.lololo	sex gif
229.3 kB	https://koodous.com/apks/8d1850d561ad9486ef2a028a70348620b2f24a9d5a932bc49cccc21118bbddfe	ea72569044cea5ad7053398dd865ca0f	com.lololo	Munisa Rizayeva
3.5 MB	https://koodous.com/apks/014e1753f2f1a3c1685297048a416bd40d728979bf5f41fa7332bb60c1aee72f	727b985e8652db6b919f75a4bf6b2daa	com.lololo	Новороссия - новости Донбасса
187.4 kB	https://koodous.com/apks/64710ec94f29be6d1cd904971292d9f18099846072d8bcf617027bb49ed56083	a4ee2c5b1efbf331eb61f489a44d465e	com.lololo	Yolğon dastur tuzish
87.8 kB	https://koodous.com/apks/c99ddc494041cdd20e61a686149e70579c6712714d635f73b630bf5a98456237	96b0b04530cdff5401432d4bab53885a	com.lololo	Новороссия - новости Донбасса
12.7 MB	https://koodous.com/apks/6ba6fbc6fd4313c5908e7331fbe8f273448f18df94243059ffb63ffaba3c2b23	8fbecd29156df4a3f754994a0d6e70f4	com.lololo	Новороссия - новости Донбасса
1.0 MB	https://koodous.com/apks/94ff218baf9689f4a1721ba9d86d6744ce3055d6403cda6bd411c3a1983cbfda	4a9a498594f7a6dceccfba88a78a30ca	com.lololo	Взлом Wi-Fi, страниц Вк, и онлайн игр
193.9 kB	https://koodous.com/apks/449a754d726c6b6e49f8e532ac580f8a830b8db5e96bdf788c7f41dfb53e12c3	889b49d50573e79163c62bd83ba539d1	com.lololo	FREE NET
193.9 kB	https://koodous.com/apks/35527f9a6cf20f1c8a061bd5ee7cf99ed50c5b861b14692ecd7b74fae3538908	e743b231771f7c65ed9fd7231f43ecb0	com.lololo	FREE NET
193.9	https://koodous.com/apks/6c44410	1c4e80f3442609ecc81f14	com.lololo	FREE NET

kB	b5e7527e4f81a8302216675c1b79518d25d6955ece54d667c1ab93594	48afffd90a		
193.9 kB	https://koodous.com/apks/a2ef2be0ebe12a5c3d9a61d1b65a7b83763b36c77d6e9987c576e6bd9dcc7354	8e6aeac68a6c9792064fa937fe6365c7	com.lololo	FREE NET
198.7 kB	https://koodous.com/apks/3f82bf9ea56775bd085821f0b355ded14fa6ddd75506d9dd386d54233fd6eb80	2b7bb30972aaeec666cb811a182db113	com.lololo	Chest Clash Royal
199.0 kB	https://koodous.com/apks/ad3b2b6d1279d2b5cf3d2e45b5c8c5a9b9c2ba1552e38d22fd166723ff0cd36e	40cfd2687a189a58135900adbc4d105f	com.lololo	Chest Clash Royal
197.2 kB	https://koodous.com/apks/54e0cf51c870e626f1c53f5ace6fb25cc28b0b3fa36fa6391ecb24361ee28d0f	a6625ad1257fdaab53da02ac92910cc5	com.lololo	Clash Royal Chest
462.8 kB	https://koodous.com/apks/8e59b55af0c8f54aeb04f09104a64f92c42854675a26f0e8679d0a6e8584d8d9	0ffb6ddd0d89673683065e94f7476c36	com.lololo	5000 MB UCELL
193.9 kB	https://koodous.com/apks/d6b237cf3437341d41959a6e24dc641d9dd297b66f91f8db2af43fd6b35e41a0	fc408e62ab155fa6325a002c751fd4eb	com.lololo	spamdan chiqish yo'llari
193.4 kB	https://koodous.com/apks/e72c1016771152f103d3024a74e3ac4a28f7da609845667c77db467937c3d1b4	4cc10eaed9bc7e45849fbb75329b6000	com.lololo	wifiaccess2