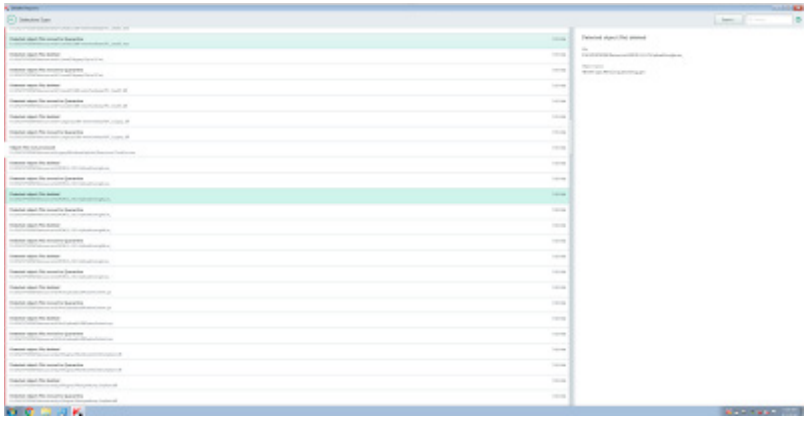
2017 年 1 月 12 日星期四

对 Shadow Brokers 恶意软件的防护

Shadow Brokers 在告别消息中发布了一系列疑似 Windows rootkit 的组件。其发布的恶意软件中包括许多可能被卡巴斯基安全产品触发为“equationdrug.generic”或“equationdrug.k”的 Windows 恶意软件文件。



这些文件的签署密钥与先前意为方程式 (Equation Group) 恶意软件的密钥相同，这表明这些文件都来自同一个威胁源。Talos 已对这些文件进行了证实，并将继续监控事态的发展，以便采取另外的措施。

IOC

fcfb56fa79d2383d34c471ef439314edc2239d632a880aa2de3cea430f6b5665
515374423b8b132258bd91acf6f29168dcc267a3f45ecb9d1fe18ee3a253195b
94c4733eebf19013df3b42d76c11ed5d153a56bdab57e1c748e07cc7da38f3ba
694be2698bcc5c7a1cce11f8ef65c1c96a883d14b98148c36b32888fb58b6a7e
0bb750195fbd93d174c2a8e20bcbcae4efefc881f7961fdca8fa6ebd68ac1edf
73d1d55493886639c619e9f5e312daab93e4feeb74f24dbe51593842baac8d15
c8b354793ad5a16744cf1d4efdc5fe48d5a0cf0657974eb7145e0088fcf609ff
e1c9c9f031d902e69e42f684ae5b35a2513f7d5f8bca83dfbab10e8de6254c78
5f06ec411f127f23add9f897dc165eaa68cbe8bb99da8f00a4a360f108bb8741
c7bf4c012293e7de56d86f4f5b4eeb6c1c5263568cc4d9863a286a86b5daf194
d382e598544a739dd17b407466a536070203cbe375c56c54792b6d0eded678cd
dfb38ed2ca3870faf351df1bd447a3dc4470ed568553bf83df07bf07967bf520
104c466732154ec25eb8b81efa88c74cec0a5baeaba76f6fd6eaa30c285c212b
d92928a867a685274b0a74ec55c0b83690fca989699310179e184e2787d47f48

0cbc5cc2e24f25cb645fb57d6088bcfb893f9eb9f27f8851503a1b33378ff22d
e44fe9432c5e11b51660efc37bf9b553260ad4130651a604ad11ca784d7f9238
339855618fb3ef53987b8c14a61bd4519b2616e766149e0c21cbd7cbe7a632c9
412efa09d71223208f3d24a661b8539d98aad6b61157707e865e288a96cda806
7352bece317e6e6896d7667faa2b38bb4f1a38112821567136d60369a91bcbef
4ebfc1f6ec6a0e68e47e5b231331470a4483184cf715a578191b91ba7c32094d
fb693eb9612d5e039a7a0fc5a183d0407cc2bce5617e7e22d2bd56caa5191e5f
27972d636b05a794d17cb3203d537bcf7c379fafd1802792e7fb8e72f130a0c4
4e0209b4f5990148f5d6dee47dbc7021bf78a782b85cef4d6c8be22d698b884f
227faeb770ba538fb85692b3dfcd00f76a0a5205d1594bd0969a1e535ee90ee1
25a2549031cb97b8a3b569b1263c903c6c0247f7fff866e7ec63f0add1b4921c
33ba9f103186b6e52d8d69499512e7fbac9096e7c5278838127488acc3b669a9
0df9d223d6bf3e1c4ba8fec7522dceb63902d1f9ddd7c26da1560da54dce2f3b
7a6488dd13936e505ec738dcc84b9fec57a5e46aab8aff59b8cfad8f599ea86a
c68f420b5a5e085a508a2529ac001284a255090920a0236df1b5656d010966e8
fe42139748c8e9ba27a812466d9395b3a0818b0cd7b41d6769cb7239e57219fb
964762416840738b1235ed4ae479a4b117b8cdcc762a6737e83bc2062c0cf236
2b27f2faae9de6330f17f60a1d19f9831336f57fdfef06c3b8876498882624a6
28a9a86f0f0a3cc4383c9f6632ee0129309afe4102d0cee1a110702a95dc0022
cdee0daa816f179e74c90c850abd427fbfe0888dcfbc38bf21173f543cdcdc66
03f22bf2f33d1032959ca68aad78ccecc201a4e5f07f446f9d1284a60fbe3361
31d86f77137f0b3697af03dd28d6552258314cecd3c1d9dc18fcf609eb24229a
7d51e97251917d5def89d77aa318f82603548afc8bde906efc1b445a47585c7b
1097e1d562341858e241f1f67788534c0e340a2dc2e75237d57e3f473e024464
c3d8ffbb4ecdf6486da175e5381e855d8224acd339199c1057846bd5b74badac
53ecd7b9879f12d17c88089fcf796c85ca29ea4639e34b8ca96819517c2a059a
b7902809a15c4c3864a14f009768693c66f9e9234204b873d29a87f4c3009a50
2a1f2034e80421359e3bf65cbd12a55a95bd00f2eb86cf2c2d287711ee1d56ad
e1dff24af5bfc991dca21b4e3a19ffbc069176d674179eef691afc6b1ac6f805
8f5b97124de9fce16e2cfecb7dd2e171824c9e07546db7b3bee7c5f2c92ceda9
25eec68fc9f0d8d1b5d72c9eae7bee29035918e9dcbeab13e276dec4b2ad2a56
9191e9bc8b64af9545b0e6e2ac022ad20b7905a6b327f768d822ff62233f3726
7b4986aee8f5c4dca255431902907b36408f528f6c0f7d7fa21f079fa0a42e09
ef906b8a8ad9dca7407e0a467b32d7f7cf32814210964be2bfb5b0e6d2ca1998
69dcc150468f7707cc8ef618a4cea4643a817171babfba9290395ada9611c63c
9022a6ece80e75a58a7e41b44aa27497ea3f8e4713c0af5e0887d60cde1fe3ba
26215bc56dc31d2466d72f1f4e1b6388e62606e9949bc41c28968fcb9a9d60a6
b2daf9058fdc5e2affd5a409aebb90343ddde4239331d3de8edabeafdb3a48fa
137749c0fbb8c12d1a650f0bfc73be2739ff084165d02e4cb68c6496d828bf1d
45e5e1ea3456d7852f5c610c7f4447776b9f15b56df7e3a53d57996123e0cebf
4254ee5e688fc09bdc72bcc9c51b1524a2bb25a9fb841feaf03bc7ec1a9975bf
f7a886ee10ee6f9c6be48c20f370514be62a3fd2da828b0dff44ff3d485ff5c5

aadfa0b1aec4456b10e4fb82f5cfa918dbf4e87d19a02bcc576ac499dda0fb68
00f782e2d4b901f0d860c3da00e154d5f0ccaf2fe758c61a27b1c0a85a927a34
dfd5768a4825d1c7329c2e262fde27e2b3d9c810653585b058fcf9efa9815964
fda57a2ba99bc610d3ff71b2d0ea2829915eabca168df99709a8fdd24288c5e5
12c082f74c0916a0e926488642236de3a12072a18d29c97bead15bb301f4b3f8

发布者：EARL CARTER；发布时间：0:33
标签：恶意软件、SHADOW BROKERS、WINDOWS

分享此文