Indicator type	Indicator
YARA	30c438fd29c43a0faf9760b600695961f520d585
FileHash-SHA256	4a25d98c121bb3bd5b54e0b6a5348f7b09966bffeec30776e5a731813f05d49e
YARA	4a2b87a5bb6c5170d4145d05b20e80b2b902d5c2
YARA	4c521ecbef4740c116d45818ebc5e35aa6aa2074
FileHash-MD5	509c41ec97bb81b0567b059aa2f50fe8
YARA	50ba934eac8d6dd4f2da24a1bb62dcf61ed27006
FileHash-SHA256	51432d3196d9b78bdc9867a77d601caffd4adaa66dcac944a5ba0b3112bbea3b
FileHash-SHA1	571dfbe51a38dc94585a2f35c9b4e426d187a0f3
domain	57g7spgrzlojinas.onion
FileHash-SHA1	61b9ae415fbe95bf4e6c616ce433cd20dce7dfe3
FileHash-MD5	61c0b4ab71713f213427aaba7524ee26
FileHash-MD5	63446bef3c45ca34c91d956a98182b40
YARA	65d94377a0ab026c53bd40f0d6a596eee34d8291
FileHash-SHA1	69ac81a5f69653ac16be7d95e736816902813e85
domain	76jdd2ir2embyv47.onion
FileHash-MD5	7b8649571847cedf86f708eefad9f640
FileHash-MD5	7bf2b57f2a205768755c07f238fb32cc
YARA	7cb27220ed0430290482a831a96320df7424f2c9
FileHash-MD5	7de2e4f0db359886a8875faa982ad515
FileHash-MD5	80ce983d22c6213f35867053bec1c293
YARA	83d956e0a64859d4229e6090454dc2efb76f7593
YARA	8fc6019e6a920ceed7fb81219cadd41afb998464
FileHash-SHA1	90873b0d61ab387d4f95a79407a0bdec7ff06896
YARA	9a95541b6b9e99c9f74eab8c77ba8c62501939de
FileHash-SHA256	a02748c3078a897cff8c4c66292662712d62e39b580465251bca6851ab6931a3
FileHash-SHA256	a4915232a46759dd27bd939e5a9161571a5e00038e4f2bd95c6b2213edf09b38
FileHash-SHA256	a74783bb813b2e053013a8ac9afdc89d250c2c086bbe9f793bec6b64bb95c9f4
FileHash-SHA1	af7db69cbaa6ab3e4730af8763ae4bf7b7c0c9b2
YARA	b123442a7dbe071d66679bd7b6204f30926af9ca
FileHash-SHA1	b9ce098e5172542fc9c76d62848b2e9291af46be
FilePath	C:\Windows\mssecsvc.exe
FilePath	C:\WINDOWS\tasksche.exe
YARA	c28ed3ca3cc3d023d1725936534965abc6f23f4e
FileHash-SHA1	c5e6c97e27331b6d38717e156ba89df1387d94f7
CVE	CVE-2017-0144
CVE	CVE-2017-0147
domain	cwwnhwhlz52maqm7.onion
YARA	dee6c8cad572727e66d2cbab3022514d310418c1
FileHash-SHA256	f01b7f52e3cb64f01ddc248eb6ae871775ef7cb4297eba5d230d0345af9a5077
YARA	faf91883526f976359044adbf12b7db0c1a4e53d
domain	gx7ekbenv2riucmf.onion
domain	iuqerfsodp9ifjaposdfjhgosurijfaewrwergweb.com
domain	iuqssfsodp9ifjaposdfjhgosurijfaewrwergwea.com
domain	sqjolphimrr7jqw6.onion
hostname	www.ayylmaotjhsstasdfasdfasdfasdfasdfasdf.com
hostname	www.idlercwww.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com