ID: [GOV-CERT#20170627-01]

27.06.2017

ГосСОПКА

КРИПТОЛОКЕР НА ОСНОВЕ СВЯЗКИ PETYA/MISHA

НОВАЯ ВОЛНА ЗАРАЖЕНИЙ ТРОЯНАМИ-ВЫМОГАТЕЛЯМИ

ransomware, cryptolocker, trojan, шифровальщик, вымогатель, EternalBlue

TLP: WHITE

E-MAIL: GOV-CERT@GOV-CERT.RU

Уровень угрозы: Высокий

Зафиксирована масштабная кампания по заражению компьютеров под управлением ОС Microsoft Windows вирусом-вымогателем на основе комбинации криптолокеров Petya/Misha. ВПО способно шифровать не только сами пользовательские файлы, но и главную файловую таблицу (MFT). Первичное заражение происходит через фишинговые письма (CVE-2017-0199), дальнейшее распространение – через эксплоит EternalBlue к уязвимости SMB v.1 CVE-2017-0144 (MS17-010).

Цели	Наибольшее распространение в нефтехимической и энергетической отраслях, а также банковском и ритейлинговом секторах экономики России и зарубежья.
Время	С 27.06.2017 по н/в
Реализация	Вектор внедрения: целевой фишинг. Вектор распространения: SMB v.1 (445 порт); удаленный доступ к консоли WMI (Windows Management Instrumentation); вероятно использование утилиты «PSEXEC». ВПО состоит из двух компонентов: модифицированной версии высокоуровневого криптолокера Misha и низкоуровневого Petya. Дроппер пытается получить права Администратора системы, используя всплывающее окно UAC или использует техники его обхода при помощи Misha. Не получив административного доступа Misha шифрует пользовательские файлы. В случае получения прав Администратора программа перезаписывает MBR, устанавливая низкоуровневый криптолокер Petya. Последний вызывает падение системы и, после её перезагрузки пользователем, имитирует работу программы CHKDSK, шифруя MFT. По завершении шифрования пользователю предлагается внести выкуп за расшифровку диска.

Противодействие	1.	Обновление ОС Windows и баз АВС.
	2.	Закрытие TCP-порта 445.
	3.	В некоторых случаях может оказаться эффективной защита MBR от перезаписи.
	4.	Заблокировать запуск ПО «PSEXEC.EXE» на потенциально уязвимых машинах.
	5.	В качестве временной меры – отключить удаленный доступ к WMI.

Индикаторы	SHA256:	17dacedb6f0379a65160d73c0ae3aa1f03465ae75cb6ae754c7dcb3017af1fbd	
	MD5:	71b6a493388e7d0b40c83ce903bc6b04	
	SHA1:	34f917aaba5684fbe56d3c57d48ef2a1aa7cf06d	
	SHA256:	027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745	
	MD5:	415fe69bf32634ca98fa07633f4118e1	Фишинговый документ
	SHA1:	101cc1cb56c407d5b9149f2c3b8523350d23ba84	Фишинговый документ
	SHA256:	Fe2e5d0543b4c8769e401ec216d78a5a3547dfd426fd47e097df04a5f7d6d206	Фишинговый документ
	MD5:	0487382a4daf8eb9660f1c67e30f8b25	
	SHA1:	736752744122a0b5ee4b95ddad634dd225dc0f73	
	SHA256:	Ee29b9c01318a1e23836b949942db14d4811246fdae2f41df9f0dcd922c63bc6	
	MD5:	A1d5895f85751dfe67d19cccb51b051a	
	MD5:	0df7179693755b810403a972f4466afb	
	MD5:	42b2ff216d14c2c8387c8eabfb1ab7d0	
	MD5:	E595c02185d8e12be347915865270cca	
	MD5:	e285b6ce047015943e685e6638bd837e	
	SHA1:	9288fb8e96d419586fc8c595dd95353d48e8a060	Дроппер
	SHA1:	a809a63bc5e31670ff117d838522dec433f74bee	Дроппер
	SHA1:	d5bf3f100e7dbcc434d7c58ebf64052329a60fc2	Дроппер

SHA1:	aba7aa41057c8a6b184ba5776c20f7e8fc97c657	Дроппер
SHA1:	bec678164cedea578a7aff4589018fa41551c27f	Дроппер
SHA1:	078de2dc59ce59f503c63bd61f1ef8353dc7cf5f	Дроппер
SHA1:	0ff07caedad54c9b65e5873ac2d81b3126754aac	Дроппер
SHA1:	51eafbb626103765d3aedfd098b94d0e77de1196	Дроппер
SHA1:	82920a2ad0138a2a8efc744ae5849c6dde6b435d	Дроппер
SHA1:	1b83c00143a1bb2bf16b46c01f36d53fb66f82b5	Дроппер
SHA1:	7ca37b86f4acc702f108449c391dd2485b5ca18c	Дроппер
SHA1:	2bc182f04b935c7e358ed9c9e6df09ae6af47168	Дроппер
SHA256:	027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745	
SHA1:	9288fb8e96d419586fc8c595dd95353d48e8a060	
SHA1:	17dacedb6f0379a65160d73c0ae3aa1f03465ae75cb6ae754c7dcb3017af1fbd	
SHA256:	64b0b58a2c030c77fdb2b537b2fcc4af432bc55ffb36599a31d418c7c69e94b1	Petya sample
SHA256:	027cc450ef5f8c5f653329641ec1fed91f694e0d229928963b30f6b0d7d3a745	Petya sample
Filename:	%WINDIR%\perfc.dat	
Filename:	C:\myguy.xls.hta	
Filename:	dllhost.dat	
Filename:	%APPDATA%\10807.exe	

Yara-правила	rule ransomware_PetrWrap { meta: copyright = "Kaspersky Lab" description = "Rule to detect PetrWrap ransomware samples" last_modified = "2017-06-27" author = "Kaspersky Lab" hash = "71B6A493388E7D0B40C83CE903BC6B04" version = "1.0" strings: $a1 = "MIIBCgKCAQEAxP/VqKc0yLe9JhVqFMQGwUITO6WpXWnKSNQAYT0O65Cr8PjIQInTeHkXEjfO2n2JmURWV/uHB 0ZrlQ/wcYJBwLhQ9EqJ3iDqmN19Oo7NtyEUmbYmopcq+YLIBZzQ2ZTK0A2DtX4GRKxEEFLCy7vP12EYOPXknVy/+ mf0JFWixz29QiTf5oLu15wVLONCuEibGaNNpgq+CXsPwfITDbDDmdrRIiUEUw6o3pt5pNOskfOJbMan2TZu" fullword wide $a2 = ".3ds.7z.accdb.ai.asp.aspx.avhd.back.bak.c.cfg.conf.cpp.cs.ctl.dbf.disk.djvu.doc.docx.dwg.eml.fdb.gz.h.hdd.kdbx.m ail.mdb.msg.nrg.ora.ost.ova.ovf.pdf.php.pmf.ppt.pptx.pst.pvi.py.pyc.rar.rtf.sln.sql.tar.vbox.vbs.vcb.vdi.vfd.vmc.vm dk.vmsd.vmx.vsdx.vsv.work.xls" fullword wide $a3 = "DESTROY ALL OF YOUR DATA! PLEASE ENSURE THAT YOUR POWER CABLE IS PLUGGED" fullword ascii $a4 = "1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX" fullword ascii $a5 = "wowsmith123456@posteo.net." fullword wide condition: uint16(0) == 0x5A4D and filesize < 1000000 and any of them }

Сигнатуры Snort	alert tcp any any -> $HOME_NET 445 (msg: "[PT Open] Unimplemented Trans2 Sub-Command code. Possible ETERNALBLUE (WannaCry, Petya) tool"; flow: to_server, established; content: "|FF|SMB2|00 00 00 00|"; depth: 9; offset: 4; byte_test: 2, >, 0x0008, 52, relative, little; pcre: "/\xFFSMB2\x00\x00\x00\x00.{52}(?:\x04|\x09|\x0A|\x0B|\x0C|\x0E|\x11)\x00/"; flowbits: set, SMB.Trans2.SubCommand.Unimplemented; reference: url, msdn.microsoft.com/en-us/library/ee441654.aspx; classtype: attempted-admin; sid: 10001254; rev: 2;) alert tcp any any -> $HOME_NET 445 (msg: "[PT Open] ETERNALBLUE (WannaCry, Petya) SMB MS Windows RCE"; flow: to_server, established; content: "|FF|SMB3|00 00 00 00|"; depth: 9; offset: 4; flowbits: isset, SMB.Trans2.SubCommand.Unimplemented.Code0E; threshold: type limit, track by_src, seconds 60, count 1; reference: cve, 2017-0144; classtype: attempted-admin; sid: 10001255; rev: 3;) alert tcp any any -> $HOME_NET 445 (msg: "[PT Open] Trans2 Sub-Command 0x0E. Likely ETERNALBLUE (WannaCry, Petya) tool"; flow: to_server, established; content: "|FF|SMB2|00 00 00 00|"; depth: 9; offset: 4; content: "|0E 00|"; distance: 52; within: 2; flowbits: set, SMB.Trans2.SubCommand.Unimplemented.Code0E; reference: url, msdn.microsoft.com/en-us/library/ee441654.aspx; classtype: attempted-admin; sid: 10001256; rev: 2;) alert tcp any any -> $HOME_NET 445 (msg: "[PT Open] Petya ransomware perfc.dat component"; flow: to_server, established, no_stream; content: "|fe 53 4d 42|"; offset: 4; depth: 4; content: "|05 00|"; offset: 16; depth: 2; byte_jump: 2, 112, little, from_beginning, post_offset 4; content: "|70 00 65 00 72 00 66 00 63 00 2e 00 64 00 61 00 74 00|"; distance:0; classtype:suspicious-filename-detect; sid: 10001443; rev: 1;) alert tcp any any -> $HOME_NET 445 (msg:"[PT Open] SMB2 Create PSEXESVC.EXE"; flow:to_server, established, no_stream; content: "|fe 53 4d 42|"; offset: 4; depth: 4; content: "|05 00|"; offset: 16; depth: 2; byte_jump: 2, 112, little, from_beginning, post_offset 4; content:"|50 00 53 00 45 00 58 00 45 00 53 00 56 00 43 00 2e 00 45 00 58 00 45|"; distance:0; classtype:suspicious-filename-detect; sid: 10001444; rev:1;)