ID: [GOV-CERT#20171025-01]

25.10.2017

v. 1.0

ГОССОПКА

КРИПТОЛОКЕР «BADRABBIT»

ОЧЕРЕДНАЯ МАСШТАБНАЯ АТАКА С ИСПОЛЬЗОВАНИЕМ ВИРУСА-ШИФРОВАЛЬЩИКА

ransomware, cryptolocker, шифровальщик, вымогатель, Bad_Rabbit

TLP: WHITE

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

Уровень угрозы:	Высокий

24 октября 2017 года многочисленными источниками зафиксирована масштабная кампания по заражению компьютеров под управлением ОС Microsoft Windows шифровальщиком «BadRabbit». Ряд информационных источников связывает текущую вирусную атаку с июньской эпидемией ВПО, получившего впоследствии название NotPetya (см. бюллетень [GOV-CERT#20170627-01]). Как и в случае с NotPetya, ВПО шифрует не только пользовательские файлы, но и сам диск. Вектор заражения – скомпрометированные легитимные веб-сайты.

Цели	Круг потенциальных целей атаки не ограничен; при этом в целях широкого распространения ВПО был скомпрометирован ряд информационных ресурсов СМИ.
Время	С 24.10.2017 по н/в
Реализация	Вектор внедрения: 1 этап. Watering hole – размещение ВПО на скомпрометированные легитимные веб-сайты под видом обновления для Adobe Flash Player. Перечень известных скомпрометированных ресурсов представлен ниже. 2 этап. Drive-by-download - перенаправление посетителей скомпрометированных веб-сайтов на ресурс, распространяющий файлы шифровальщика. 3 этап – заражение. При посещении скомпрометированного веб-сайта предварительно загруженный JavaScript демонстрирует пользователю окно, предлагающее установить поддельное обновление Adobe Flash Player. В случае запуска пользователем такого обновления происходит скачивание и запуск вредоносного файла (дроппера). После заражения ВПО повышает привилегии на локальной машине и инициирует процесс вторичного распространения по протоколу SMB, используя подобранные/извлечённые из LSASS

при помощи утилиты Mimikatz пароли, а также шифрует единым ключом пользовательские файлы с использованием алгоритма AES-128-CBC. Распространение по локальной сети происходит с использованием адреса заражённого хоста с маской сети /24.

Впоследствии ВПО шифрует диск с использованием ПО DiskCryptor и перезагружает компьютер, после чего пользователю предлагается внести выкуп за расшифровку диска и файлов.

Противодействие

1. Kill switch: создать файл C:\windows\infpub.dat и назначить ему права «только для чтения». Мера не позволит дропперу разместить в системе ключевой модуль шифровальщика.

2. Настройками групповой политики запретить хранение паролей в LSA Dump в открытом виде, а также использовать сложные пароли (ВПО использует перебор паролей по словарю).

3. Блокировать всплывающие окна в браузере.

4. Обновить антивирусные базы используемых средств антивирусной защиты.

5. Отключить удаленный доступ к WMI.

Индикаторы

MD5	FBBDC39AF1139AEBBA4DA004475E8839
MD5	4462B97E7CDD628D71C4CFECBFAC6723
MD5	898B338E7BF36729890C61DC82ACF511
MD5	0372713206250F98596C6BA38D507001
MD5	3CF8D4B728A56FD5A1AF0A0ED61F3A01
MD5	155E2F57C975341B6250490C14D1123B
MD5	0AC260D94C9130921CCB595D9F2390F6
MD5	54E383F769D5CB0D947ED175C6B3E2CE
MD5	83117B94D3FCC4A70E7143A5ADB75673
MD5:	666BDB7A745757945AD606AAEAA69C54

MD5	b14d8faf7f0cbcfad051cefe5f39645f
Domain	1dnscontrol[.]com
Domain	ftp.1dnscontrol[.]com
Domain	mail.1dnscontrol[.]com
Domain	ns1.1dnscontrol[.]com
Domain	ns2.1dnscontrol[.]com
Domain	ns3.1dnscontrol[.]com
Domain	pop.1dnscontrol[.]com
Domain	pridns.1dnscontrol[.]com
Domain	secdns1.1dnscontrol[.]com
Domain	secdns2.1dnscontrol[.]com
Domain	secdns3.1dnscontrol[.]com
Domain	secdns4.1dnscontrol[.]com
Domain	smtp.1dnscontrol[.]com
Domain	fastmonitor1[.]net
Domain	caforssztxqzf2nm[.]onion
File	dispci.exe
File	c:\windows\infpub.dat
File	c:\windows\cscc.dat
URI	1dnscontrol[.]com/test
URI	1dnscontrol[.]com/flash
URI	1dnscontrol[.]com/
URI	1dnscontrol[.]com/index.php
URI	1dnscontrol[.]com/install_flash_player.exe
URI	1dnscontrol[.]com/logo.png
URI	1dnscontrol[.]com/flash_install.php

Скомпрометированные ресурсы	URL	hxxp://argumentiru[.]com
	URL	hxxp://www.fontanka[.]ru
	URL	hxxp://grupovo[.]bg
	URL	hxxp://www.sinematurk[.]com
	URL	hxxp://www.aica.co[.]jp
	URL	hxxp://spbvoditel[.]ru
	URL	hxxp://argumenti[.]ru
	URL	hxxp://www.mediaport[.]ua
	URL	hxxp://blog.fontanka[.]ru
	URL	hxxp://an-crimea[.]ru
	URL	hxxp://www.t.ks[.]ua
	URL	hxxp://most-dnepr[.]info
	URL	hxxp://osvitaportal.com[.]ua
	URL	hxxp://www.otbrana[.]com
	URL	hxxp://calendar.fontanka[.]ru
	URL	hxxp://www.grupovo[.]bg
	URL	hxxp://www.pensionhotel[.]cz
	URL	hxxp://www.online812[.]ru
	URL	hxxp://www.imer[.]ro
	URL	hxxp://novayagazeta.spb[.]ru
	URL	hxxp://i24.com[.]ua
	URL	hxxp://bg.pensionhotel[.]com
	URL	hxxp://ankerch-crimea[.]ru