

How did the 'Flame' family of malware spread?

On Certificates, Code Signing, and Man-in-the-Middle
Adam Udi

What is Flame?

- ▶ Flame, also known as Flamer or Skywiper, is a form of Windows malware first discovered in 2012.
- ▶ On May 28 2012 Iran's 'Computer Emergency Response Team', Kaspersky Lab (of Kaspersky Antivirus), and the Cryptography and System Security (CrySyS) Lab at Budapest University announced the existence of a new malware which, according to CrySyS, is 'arguably the most complex malware ever found.'



What can it do?

- ▶ About 20x as large as Stuxnet, Flame has over twenty modules with many capabilities
 - ▶ Record Network traffic, keystrokes, audio, take screenshots, and even record Skype conversations
 - ▶ Turn computers into Bluetooth devices which then scan the area and attempt to download contacts from other Bluetooth devices
 - ▶ Scan a local computer for documents of interest
 - ▶ And, of course, send all this information around the world (through a network of over 60 proxies) to end up on some remote server...somewhere
- ▶ Perhaps most importantly, Flame can spread itself via either USB, or using Windows Update



How does Flame trick Windows Update?

- ▶ It all comes down to this: Microsoft made a mistake.
- ▶ In 2008 researchers at Cal Berkeley rendered useless the MD5 hash function using a cluster of 200 PlayStation 3 consoles.
 - ▶ As a result, MD5 was labeled 'cryptographically broken'
- ▶ Unfortunately, someone at Microsoft dropped the ball. One of their certificate authorities (more to come on this), a code signing authority no less, was still using MD5 come 2010 when many people believe Flame was widely distributed.



How does signing work?



“Hey, can you send me my banking information, make sure to sign it so I know someone isn’t lying to me!”






What does Bob do?

Alice's
Bank
Statement

Hash
0101
001010

Signature:
11100
111100

Now Bob has two things
to send Alice, a message
and a signature



How does signing work?



“Hey, can you send me my banking information, make sure to sign it so I know someone isn’t lying to me!”



Alice's Bank Statement	Signature: 001011100 010111100
------------------------------	--------------------------------------



How does Alice verify?



Alice's
Bank
Statement

Hash

Hash: 010101
1001010

Hash

Ver_{PK}

101
0110

Signature:
001011100
010111100

They match! Thus,
someone with Bob's
secret key must have
signed the document!



More on Signatures

- ▶ All browsers use these signatures and a huge network of trusted certificate authorities which furnish users with an important piece of information to make signatures work.
 - ▶ What information do we need?

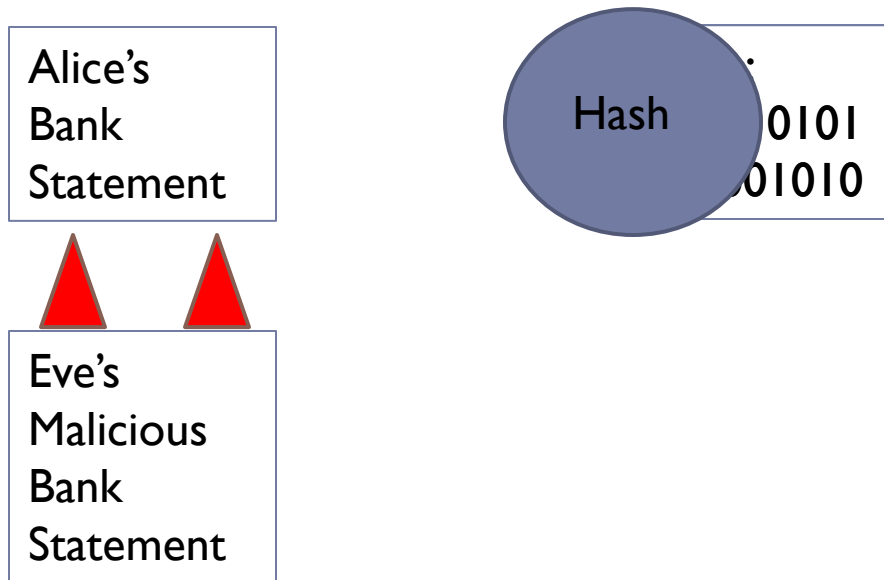


Microsoft's Signing Architecture

- ▶ Microsoft uses the same method that our browsers do to sign the code that your computer gets from Windows Update.
- ▶ There are several Certificate Authorities (CA1, CA2, CA3,...) which can sign code. These Authorities are highly regulated by Microsoft and there is a verifying process that all code must go through
- ▶ As we know, one of these authorities, which was responsible for giving out certificates which allowed arbitrary code to be signed was still using MD5, years too late.



Collision Attacks



This is the hash of
Alice's Bank
Statement

The attack on MD5 can
maliciously construct another
Bank Statement which hashes
to the same value as Alice's
statement did!



A quick aside

- ▶ An interesting note: The cryptographic guarantees given by the signature scheme were never broken... That is theoretical “security game” is still intact. It just turns out the hash function was a weak point..
- ▶ This is an example where the theoretical community and practical community have some fundamental differences when it comes to security.



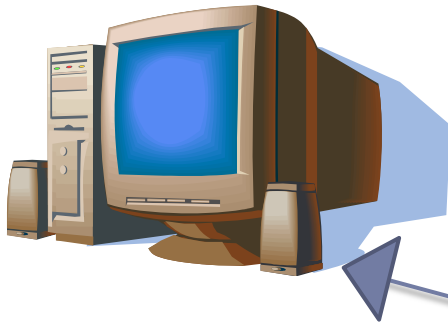
Back to Flame: Gadget and Munch

- ▶ The two modules responsible for spreading Flame on a network are called Gadget and Munch
- ▶ They use a man-in-the-middle attack to intercept Windows Update

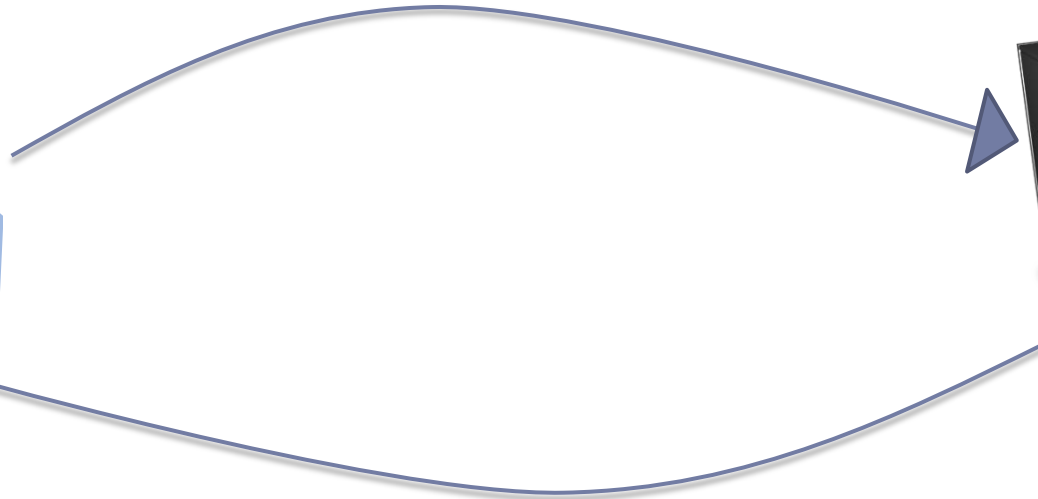


What is a Man in the Middle attack? - NORMAL

Uninfected
Computer



“Any new updates?”



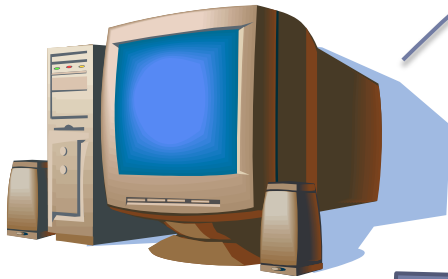
Microsoft Update Server

“Yup! Here’s the
new MSE database
updates. Signed by
Microsoft, of
course.”

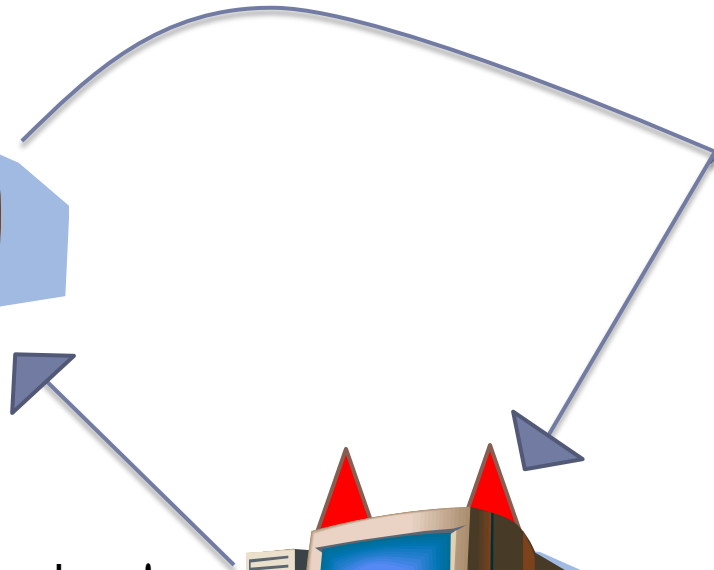


What is a Man in the Middle attack? - INFECTED

Uninfected
Computer



“Any new updates?”



“Of course we have updates!
Here’s some great code,
‘signed’ by Microsoft and
everything”



Infected
Computer

“Hmm.. I wonder where
that computer in Iraq is?
Guess it’s owner got lazy
or something...”



Microsoft Update Server



Fake Update Process

- ▶ The infected machine pretends to be a Windows Update server by announcing itself as a proxy server via “Web Proxy Autodiscovery Protocol” (WPAD)
- ▶ Any computer which finds this proxy server must simply have their proxy settings set to “Auto” (the default)



The Fake Update Process

- ▶ The fake update registers in windows update as
 - ▶ *“update description=“Allows you to display gadgets on your desktop.”
displayName=“Desktop Gadget Platform”
name=“WindowsGadgetPlatform”>*
- ▶ But it actually runs this..

```
Microsoft (R) Cabinet Tool - Version 1.00.0601 (03/18/97)
Copyright (c) Microsoft Corp 1996-1997. All rights reserved.

Listing of cabinet file '_d.cab' (size 15995):
  1 file(s), 1 folder(s), set ID 0, cabinet #0

File name           File size   Date       Time       Attrs
-----
wuSetupU.exe       29928      2011/11/01 14:03:14  -a--
```

- ▶ Which, of course, installs the rest of Flame's modules (or at least another module which downloads yet more modules)
-



Sources

- ▶ <http://arstechnica.com/discipline/hacking-2/>
- ▶ <http://arstechnica.com/security/2012/06/flame-crypto-breakthrough/>
- ▶ <http://arstechnica.com/security/2012/06/flame-wields-rare-collision-crypto-attack/>
- ▶ <http://arstechnica.com/security/2012/06/flame-malware-hijacks-windows-update-to-propagate/>
- ▶ <http://arstechnica.com/security/2012/05/spy-malware-infecting-iranian-networks-is-engineering-marvel-to-behold/>
- ▶ https://www.securelist.com/en/blog/208193558/Gadget_in_the_middle_Flame_malware_spreading_vector_identified
- ▶ <http://www.informationweek.com/security/cybercrime/flame-hits-windows-update-7-key-facts/240001490>
- ▶ <http://blogs.technet.com/b/msrc/archive/2012/06/04/security-advisory-2718704-update-to-phased-mitigation-strategy.aspx?Redirected=true>
- ▶ <http://blogs.technet.com/b/msrc/archive/2012/06/03/microsoft-releases-security-advisory-2718704.aspx>
- ▶ <http://blogs.technet.com/b/srd/archive/2012/06/03/microsoft-certification-authority-signing-certificates-added-to-the-untrusted-certificate-store.aspx>



Sources Continued

- ▶ [http://msdn.microsoft.com/en-us/library/ms537361\(v=vs.85\).aspx](http://msdn.microsoft.com/en-us/library/ms537361(v=vs.85).aspx)
- ▶ http://en.wikipedia.org/wiki/Flame_malware
- ▶ [http://www.nytimes.com/2012/05/30/world/middleeast/iran-confirms-cyber-attack-by-new-virus-called-flame.html?_r=3&hp&](http://www.nytimes.com/2012/05/30/world/middleeast/iran-confirms-cyber-attack-by-new-virus-called-flame.html?_r=3&hp&_hpid=hp)
- ▶ http://www.securelist.com/en/blog/208193522/The_Flame_Questions_and_Answers
- ▶ <http://www.crysys.hu/skywiper/skywiper.pdf>
- ▶ <http://www.kaspersky.com/flame>
- ▶ http://news.cnet.com/8301-1009_3-10129693-83.html
- ▶ http://www.securelist.com/en/blog/208193558/Gadget_in_the_middle_Flame_malware_spreading_vector_identified

