IEEE
International Conference
on
PKI and Its Applications
(PKIA-2017)
November 14-15, 2017

Hotel Chancery Pavilion, Bangalore

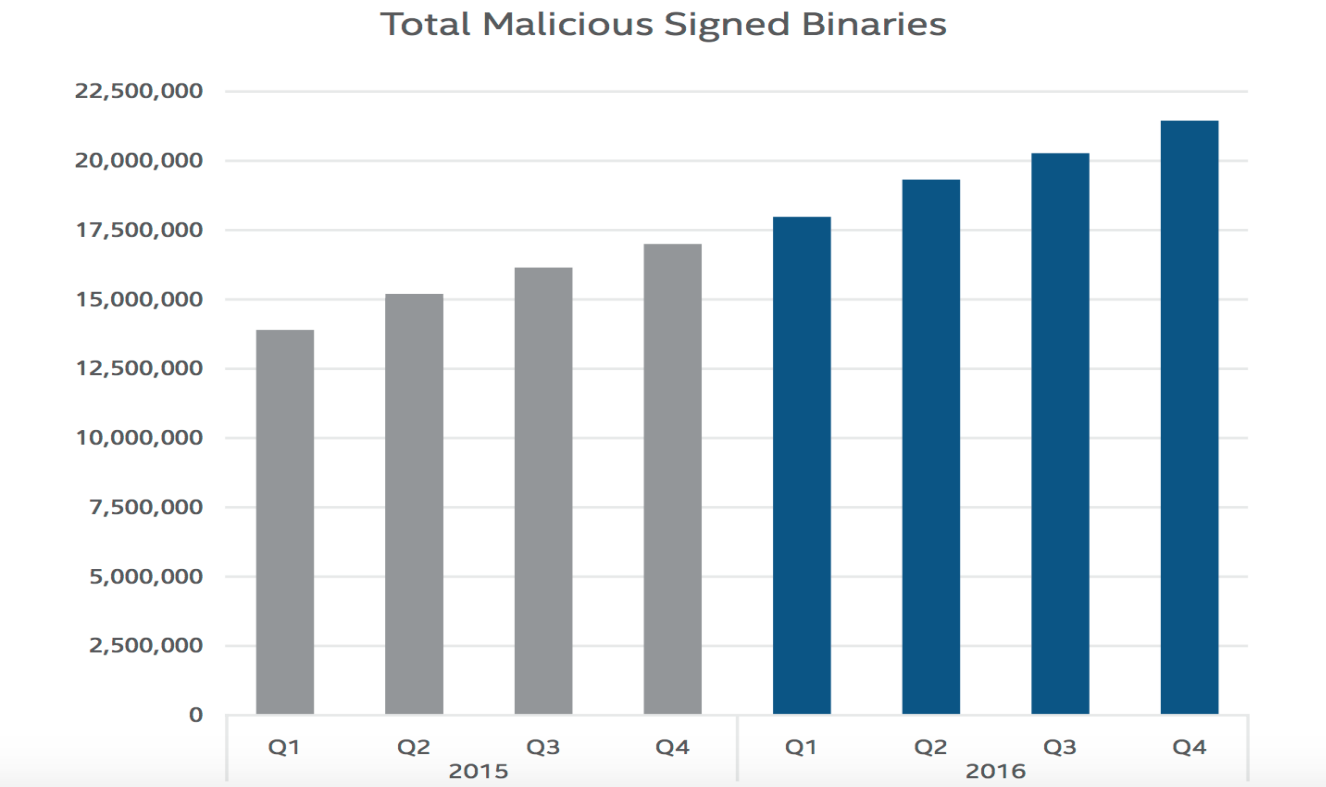
MALSIGN: THREAT ANALYSIS OF SIGNED AND IMPLICITY TRUSTED MALICIOUS CODE

Soumajit Pal, Prabaharan Poornachandran, Manu R Krishnan,
Prem Sankar AU, Parvathy Sasikala

Amrita Center for Cyber Security
Amrita University, Kerala

Signed Malware?

Image reference: [1]



Signed Binaries. Are all of them benign ?

Signed Malware contd...

Image reference: [2,3,4]

Symantec Official Blog

Suckfly: Revealing the secret life of your code signing certificates

A China-based APT group has an insatiable appetite for stolen code-signing

By: Jon_DiMaggio SYMANTEC EMPLOYEE

Created 15 Mar 2016 | 0 Comments | : 简体中文, 繁體中文, 日本語

0 | 268

Symantec Official Blog

Opera Breach - When Cybercriminals take on Targeted Attacks

By: Symantec Security Response SYMANTEC EMPLOYEE

Created 28 Jun 2013 | 0 Comments | : 日本語

0 | 6 | Like 0

On June 26 2013, browser manufacturer Opera announced that they had been breached as a resul
against their infrastructure. However, this was no ordinary targeted attack. The attackers in this ca
steal intellectual property. They wanted to use Opera's auto-update mechanism in order to propag
malware normally associated with financial Trojans.

Information Stealer - Trojan Spymel

The downloaded malware executable is a highly obfuscated .NET binary, which is digitally signed with a certificate issued to "SBO INVEST". The certificate was promptly revoked by DigiCert when notified and, therefore, is not active in any attack. We noticed a newer variant arose within two weeks of the first variant, using another certificate issued to "SBO INVEST' that is also revoked.

Digital Signature Details

General | Advanced

View Certificate

Code Signing Infrastructure: Threats

- CA side:
  - Issuing certificates to malicious groups
    - Fake companies, domains
    - VeriSign issued signing certificate to fake Microsoft employee
  - Erroneous Certificate Issue
    - TURKTRUST
    - Intermediary SSL certificates
  - Reseller Account (RA) Proxy Partner Breach
    - Commodo CA
  - Insecure Management of CA's Private Key

Code Signing Infrastructure: Threats …

- Software Provider side:
  - Insecure Infrastructure
    - Expired Opera Certificate
    - Downloader Trojan as valid Update
  - Signing unclean code
    - Adobe, compromised build server
  - Self-signed Certificates
- Client side:
  - Improper Verification of certificate
    - Certificate Revocation List (CRL)
  - User Ignorance

Meanwhile Ccleaner: “signed malware”

Monday, September 18, 2017

Security Notification for CCleaner v5.33.6162 and CCleaner Cloud v1.07.3191 for 32-bit Windows users

PAUL YUNG
VP, Products

Dear CCleaner customers, users and supporters,

We would like to apologize for a security incident that we have recently found in CCleaner version 5.33.6162 and CCleaner Cloud version 1.07.3191. A suspicious activity was identified on September 12th, 2017, where we saw an unknown IP address receiving data from software found in version 5.33.6162 of CCleaner, and CCleaner Cloud version 1.07.3191, on 32-bit Windows systems. Based on further analysis, we found that the 5.33.6162 version of CCleaner and

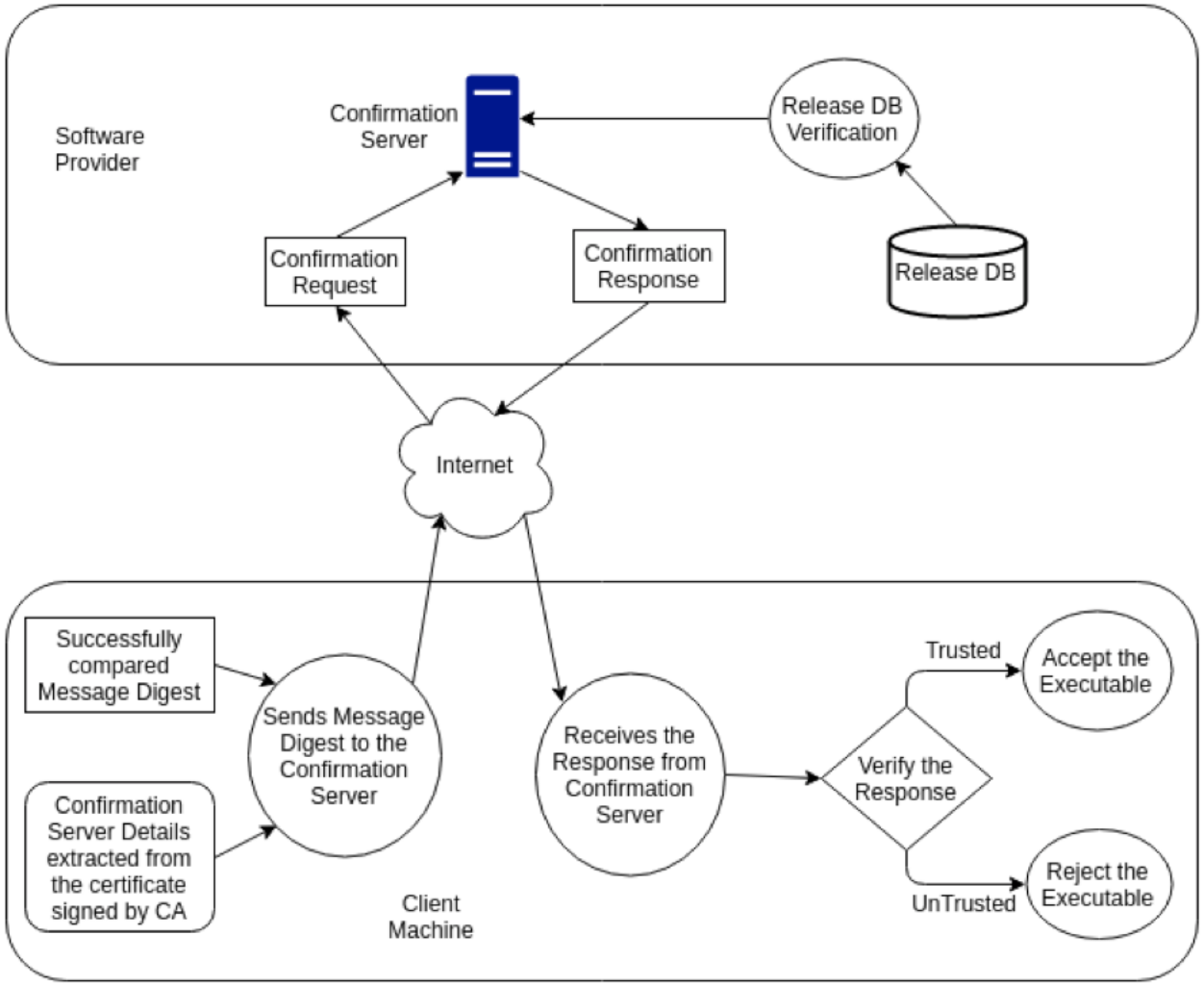
Image reference: [5]

- Compromised build server owned by Piriform ltd.
- Self-signed certificate for first stage of the attack.
- Infected app signed by valid Symantec certificate.
- Reported September 18, 2017

Tale of Signed Software Updates

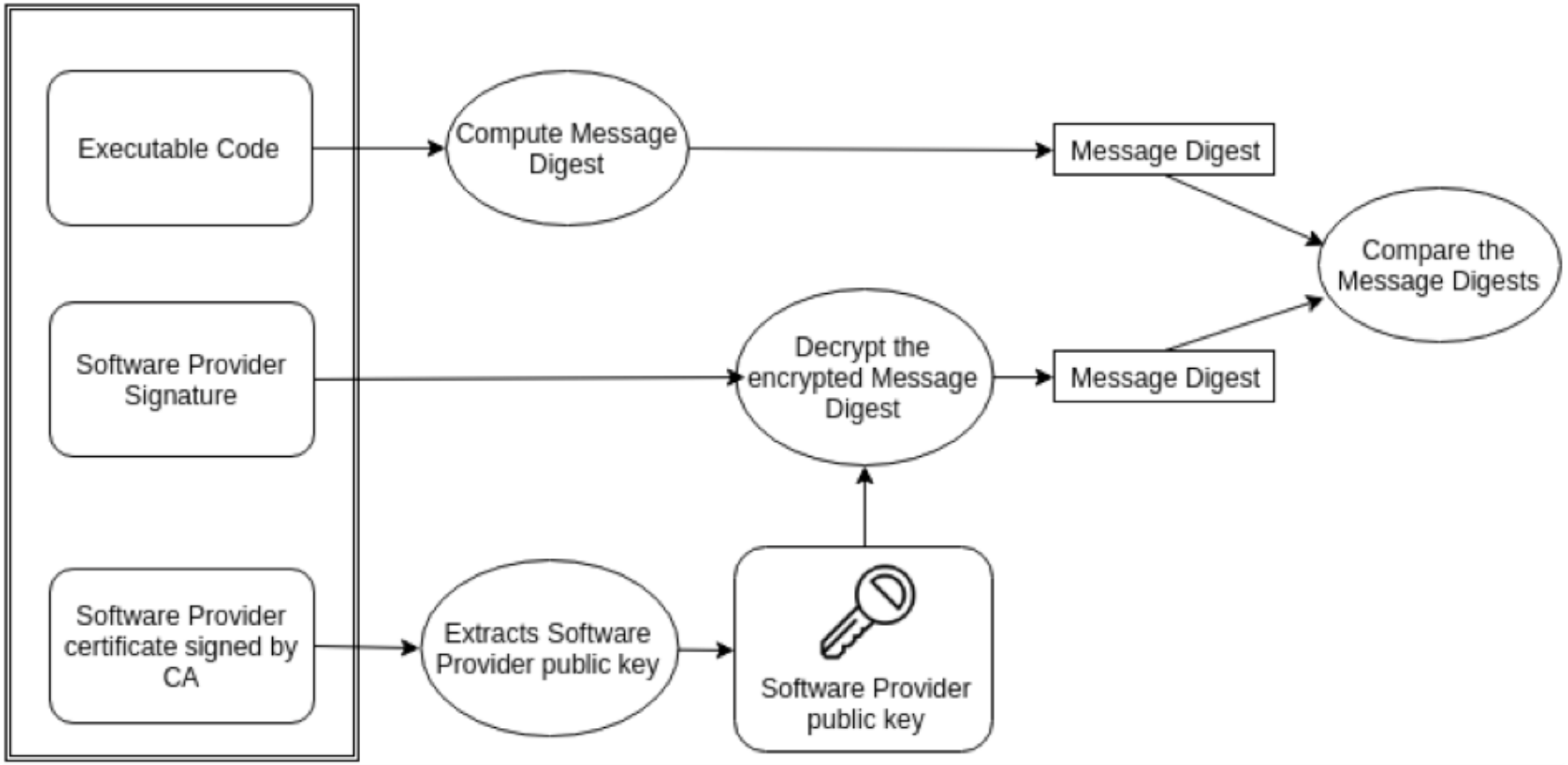
- Implicitly trusted by AV software.
- Impacted companies like Adobe, Opera ...
- Prevention mechanism?
    - Additional Security Layer
        - Works with any software update process

Secure Layer for Secure Software Updates



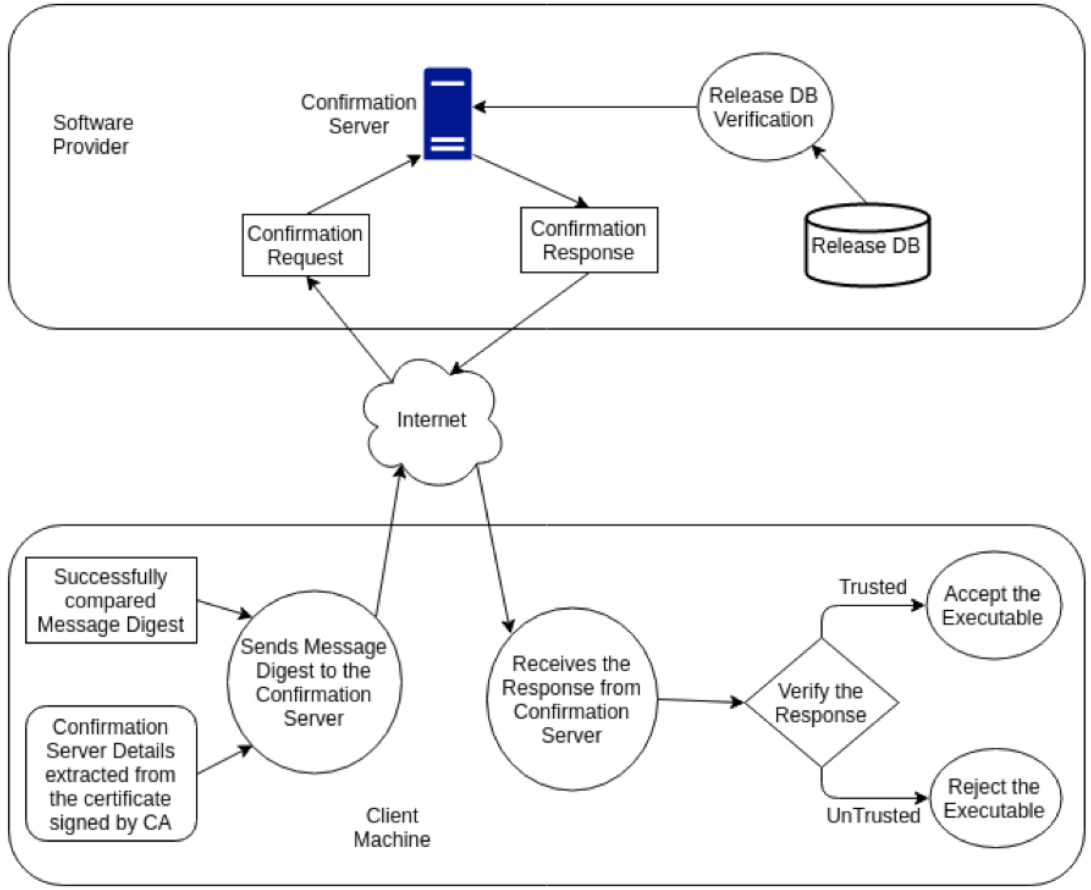
Secure Layer for Secure Software Updates

- Step 1:



Secure Layer for Secure Software Updates

- Step 2: Security Layer



Conclusion

- Impacts are manifold
  - Trust
  - Economy
  - Society
- Our model adds additional out-of-band verification which works with typical software update procedure.

References:

[1] https://www. mcafee.com/us/resources/reports/rp- quarterly- threats- mar- 2017.pdf
[2] https://www.zscaler.com/blogs/research/ yet- another- signed- malware- spymel
[3] http://www.symantec.com/connect/ blogs/opera- breach- when- cybercriminals- take- targeted- attacks
[4] https://www.symantec.com/connect/blogs/ suckfly- revealing- secret- life- your- code- signing-certificates
[5] https://www.piriform.com/news/blog/2017/9/18/security-notification-for-ccleaner-v5336162-and-ccleaner-cloud-v1073191-for-32-bit-windows-users

CCA

IEEE

PKIA-2017

Thank You

CDAC