

Session 5: Information Security



Northeastern University

International Secure Systems Lab

A Large-Scale, Automated Approach to Detecting Ransomware

Amin Kharraz

mkharraz@ccs.neu.edu

Disclosure: This research was funded by National Science Foundation
and Secure Business Austria

PRIVACYCON

Infecting Victim's Machine

Attachments



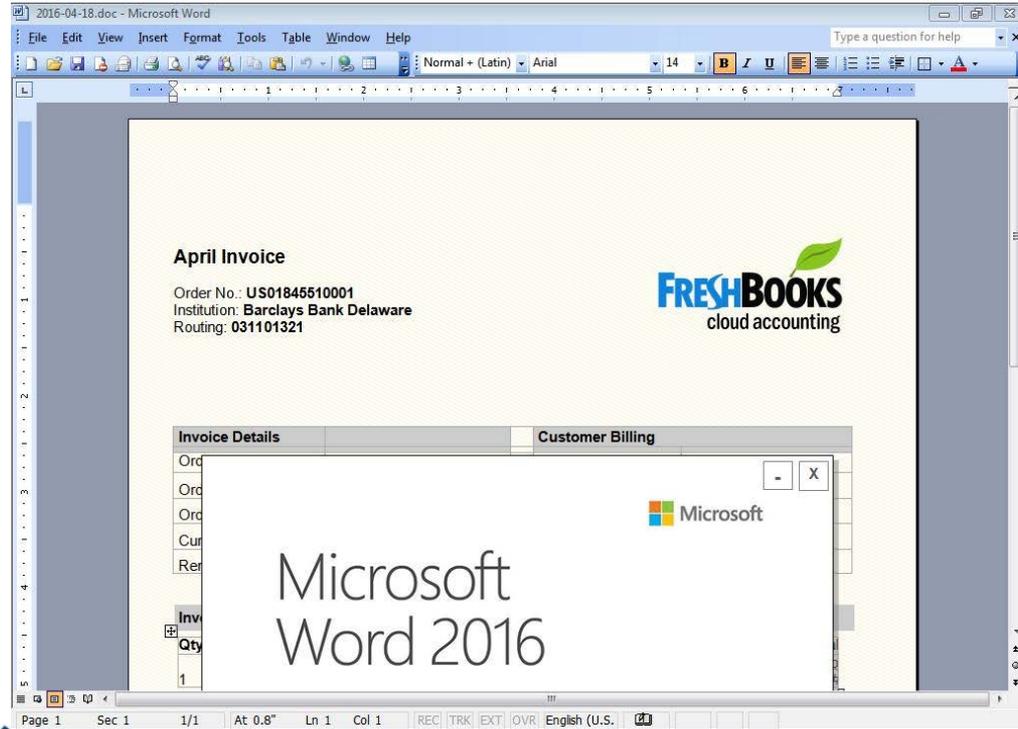
Drive-by Downloads



Malicious binaries



Macro Viruses: An Innocent Looking Word File



By opening the file you might get infected

The image shows a computer screen with a dark background. At the top, there are logos for the NSA Internet Surveillance Program, the Department of Justice, and the National Security Agency. The text reads "NSA INTERNET SURVEILLANCE PROGRAM" and "COMPUTER CRIME PROSECUTION SECTION". A large yellow "PRISM" logo is prominent. Below this, a red banner with white text says "YOUR COMPUTER HAS BEEN LOCKED!".

The main message on the screen is: "Your computer has been locked due to suspicion of illegal content downloading and distribution." It states that 414 Mb of photo and video files were classified as child pornographic materials. It lists several U.S. Federal Laws: 18 U.S.C. § 2251 (Sexual exploitation of children), 18 U.S.C. § 2252 (Certain activities relating to material involving the sexual exploitation of minors), and 18 U.S.C. § 2252A (Certain activities relating to material constituting or containing child pornography). It warns that violators may be sentenced to imprisonment from 6 months to 10 years and fined up to \$250,000.

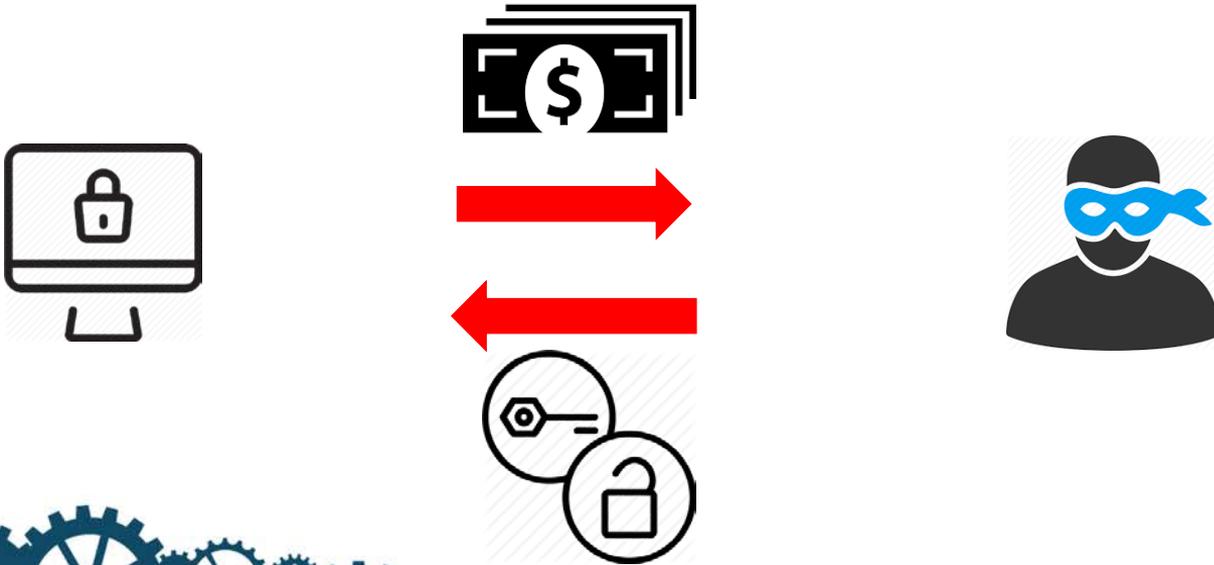
Below the laws, it says "Collected technical data" and lists: "Your IP address:", "Your host name:", "Source or intermediary sites:", and "Location:". The fields for these are redacted with black boxes.

Under "Illegal content found:", there are four small thumbnail images, all of which are redacted with black boxes.

On the right side of the screen, there is a white box with a "green dot MoneyPak" logo. It says: "Your case can be classified as occasional/unmotivated, according to 17 (U.S. Code) 5512. Thus it may be closed without prosecution. Your computer will be unlocked automatically." It offers to resolve the situation for a \$300 fine. Below this is a form to exchange cash for a MoneyPak voucher, with a "Code:" field and a "SUBMIT" button. The status is "Waiting for payment" and it says "Permanent lock on 09/28/2013 8:46 p.m. EST". At the bottom, it lists where to buy MoneyPak: Rite Aid, CVS pharmacy, Kmart, 7-Eleven, Walgreens, and Walmart.

What is a ransomware attack?

- 1 Paying the ransom fee
- 2 Receiving the decryption key



[Privacy & Security](#)

Ransomware attackers collect ransom from Kansas hospital, don't unlock all the data, then demand more money

Kansas Heart Hospital declined to pay the second ransom, saying that would not be wise. Security experts, meanwhile, are warning that ransomware attacks will only get worse.

By [Bill Siwicki](#) | May 23, 2016 | 02:58 PM

SHARE



Kansas Heart Hospital in Wichita paid the initial ransom but decided against paying the second request even though some of its data appears to still be locked.

Kansas Heart Hospital was the victim of a ransomware attack and after it paid the first one, attackers boldly demanded a second ransom to decrypt data.

Kansas Heart Hospital president Greg Duick, MD told local media that patient

University Pays \$16,000 to Stop Ransomware Attack JUNE 8, 2016

Michael Phelps Picks Up His 20th Gold in 200-Meter Butterfly 10:37 PM EDT

USA's Katie Ledecky Clinches the Gold Again in 200m Freestyle 10:17 PM EDT

Two Years After Ferguson, What Has Changed? 8:00 PM EDT

Wild and Weird, Drone Racing May be the Sport of the Future 7:57 PM EDT

Elon Musk Says SolarCity Will Sell a Roof Integrated With Solar Panels 7:56 PM EDT

Disney Hedges Its Bets on TV With BAMTech Stake and ESPN Streaming 7:06 PM EDT

TECH CHANGING FACE OF SECURITY

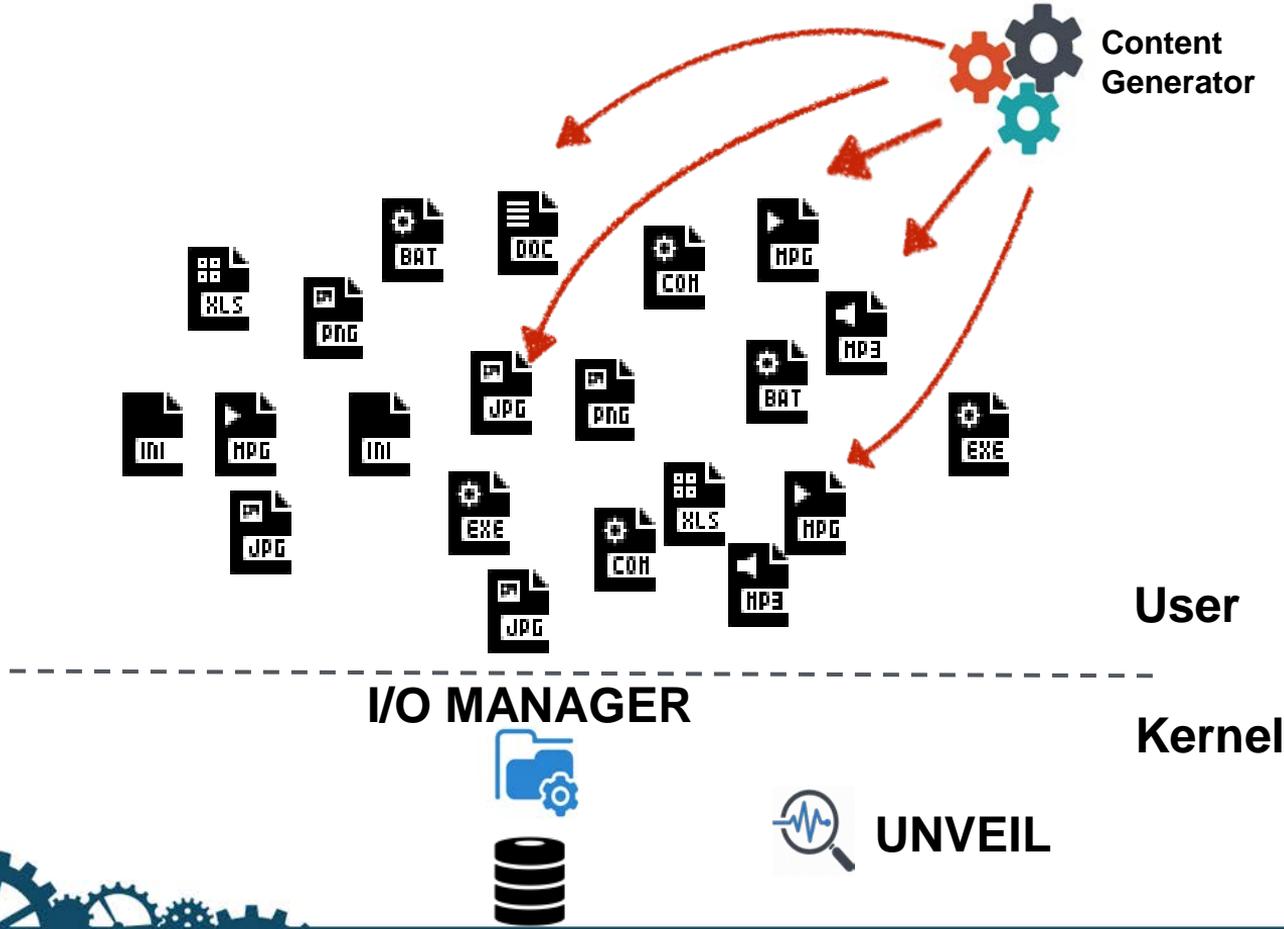
University Pays \$16,000 to Stop Ransomware Attack

by **Jeff John Roberts** @jeffjohnroberts JUNE 8, 2016, 1:29 PM EDT



Achilles' Heel of Ransomware

- Ransomware *has to inform* victim that attack has taken place
- Ransomware has certain behaviors that are predictable
 - e.g., entropy changes, modal dialogs and background activity, accessing user files
- A good sandbox that looks for some of these signs helps here...

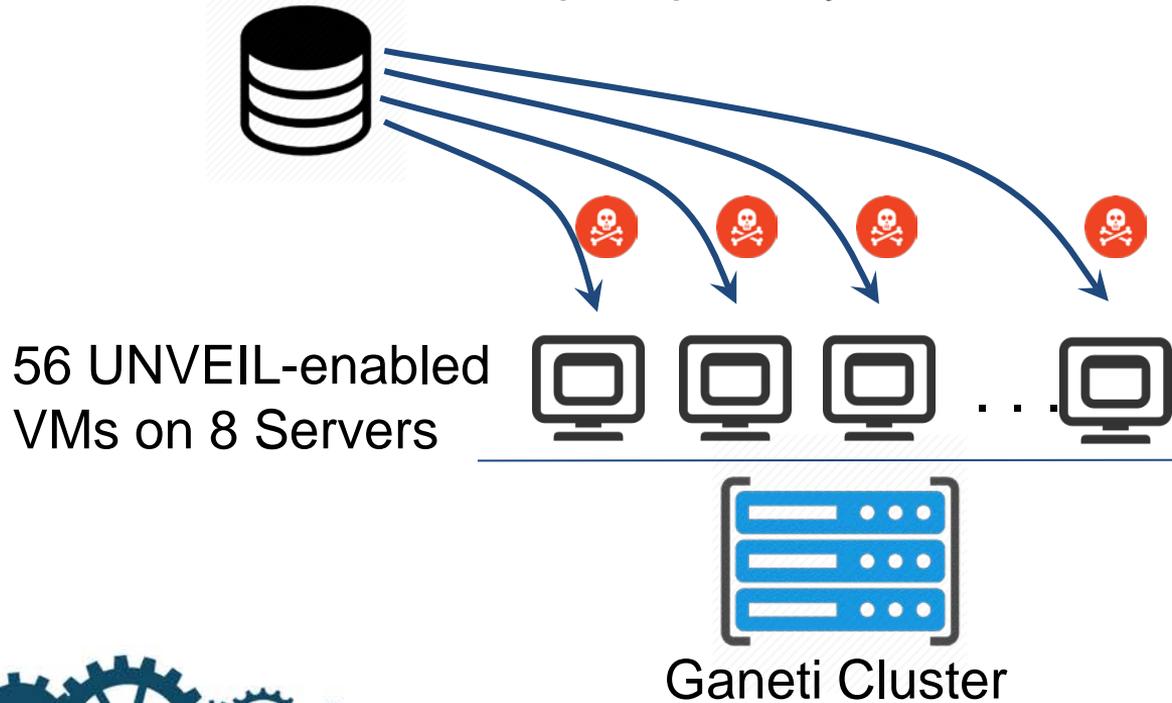


Iteration over files during a CryptoWall attack

File	Operation	Process	Entropy
midterm_paper.docx	IRP_MJ_CREATE	svchost.exe	—
midterm_paper.docx	IRP_MJ_READ	svchost.exe	4.01
midterm_paper.docx	IRP_MJ_WRITE	svchost.exe	7.28
	...		
midterm_paper.docx	IRP_MJ_CLEANUP	svchost.exe	—
midterm_paper.docx	IRP_MJ_CLOSE	svchost.exe	—
myweddingparty.mpeg	IRP_MJ_CREATE	svchost.exe	—
myweddingparty.mpeg	IRP_MJ_READ	svchost.exe	5.14
myweddingparty.mpeg	IRP_MJ_WRITE	svchost.exe	7.24
	...		
myweddingparty.mpeg	IRP_MJ_CLEANUP	svchost.exe	—
myweddingparty.mpeg	IRP_MJ_CLOSE	svchost.exe	—

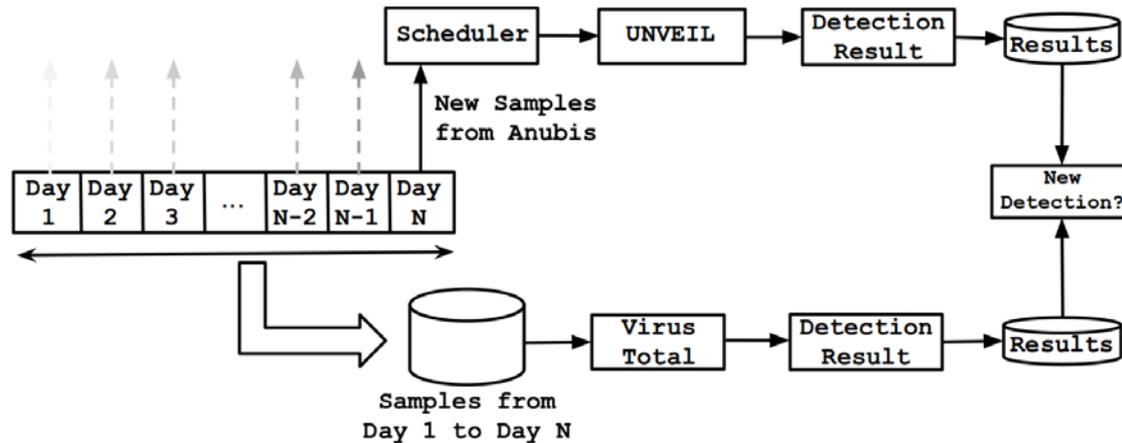
Evaluation UNVEIL with unknown samples

~ 1200 malware samples per day



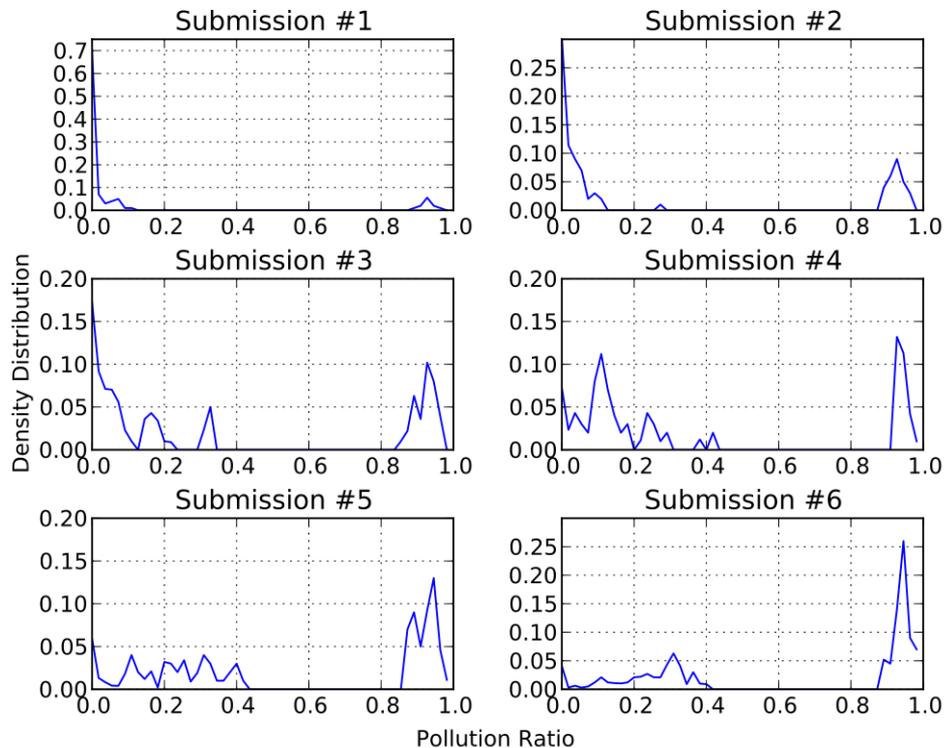
Evaluation UNVEIL with unknown samples

- The incoming samples were acquired from the daily malware feed provided by Anubis from March 18 to February 12, 2016.
- The dataset contained 148,223 distinct samples.

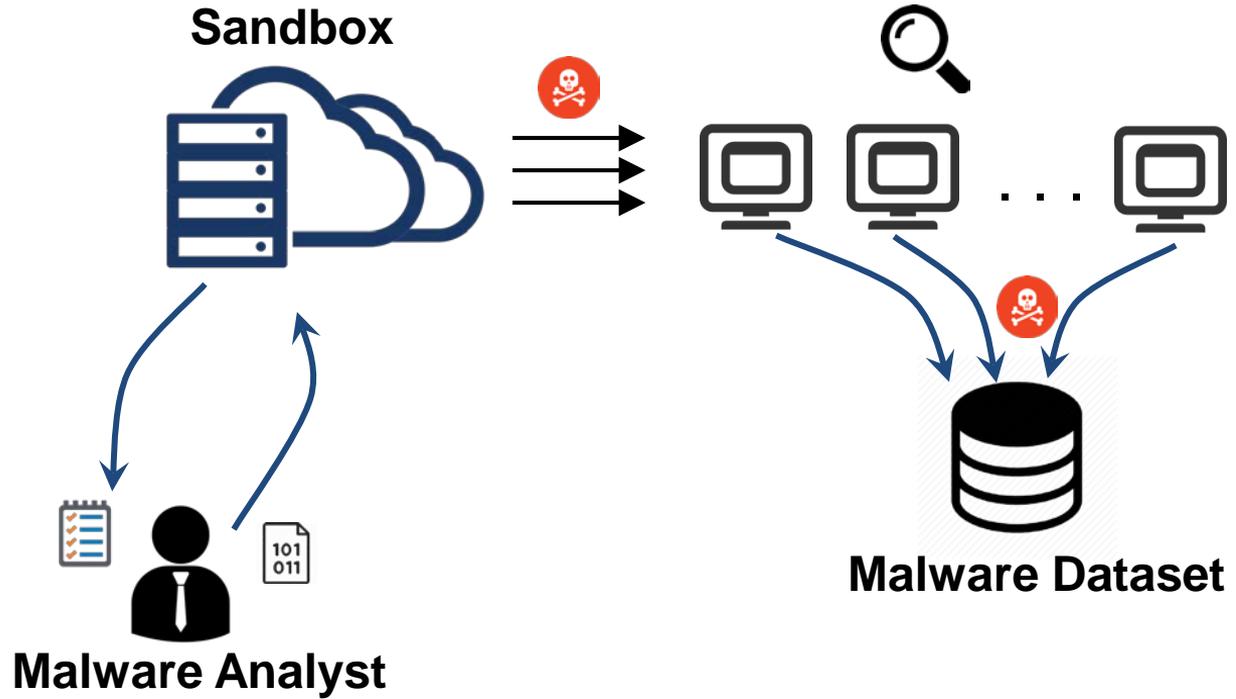


Cross-checking with VirusTotal

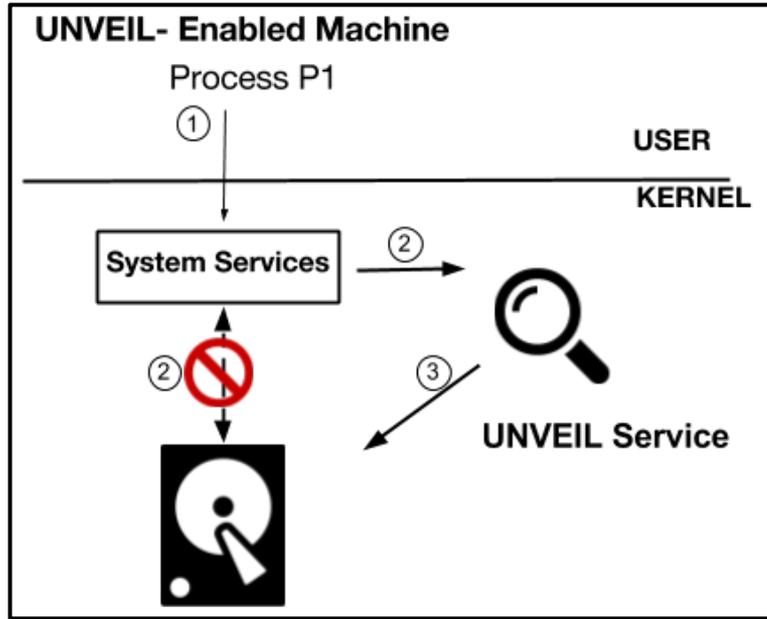
- The results are concentrated either towards small or very large detection ratios.
- A sample is either detected by a relatively small number, or almost all of the scanners.



Deployment Scenario (Malware Research)



Deployment Scenario (End-point Solution)



- Running UNVEIL as an augmented service
- UNVEIL supports legacy platforms
- Incurs modest overhead, averaging 2.6% for realistic work loads

Conclusion

- Ransomware is a challenging problem
 - But it has predictable behaviors compared to other malware
- UNVEIL introduces concrete models to detect those behaviors
 - We've shown that our detection model is useful in practice
- There is definitely room for improvement
 - We can extend our dynamic systems with functionality tuned towards detecting ransomware

Thank You



PRIVACYCON

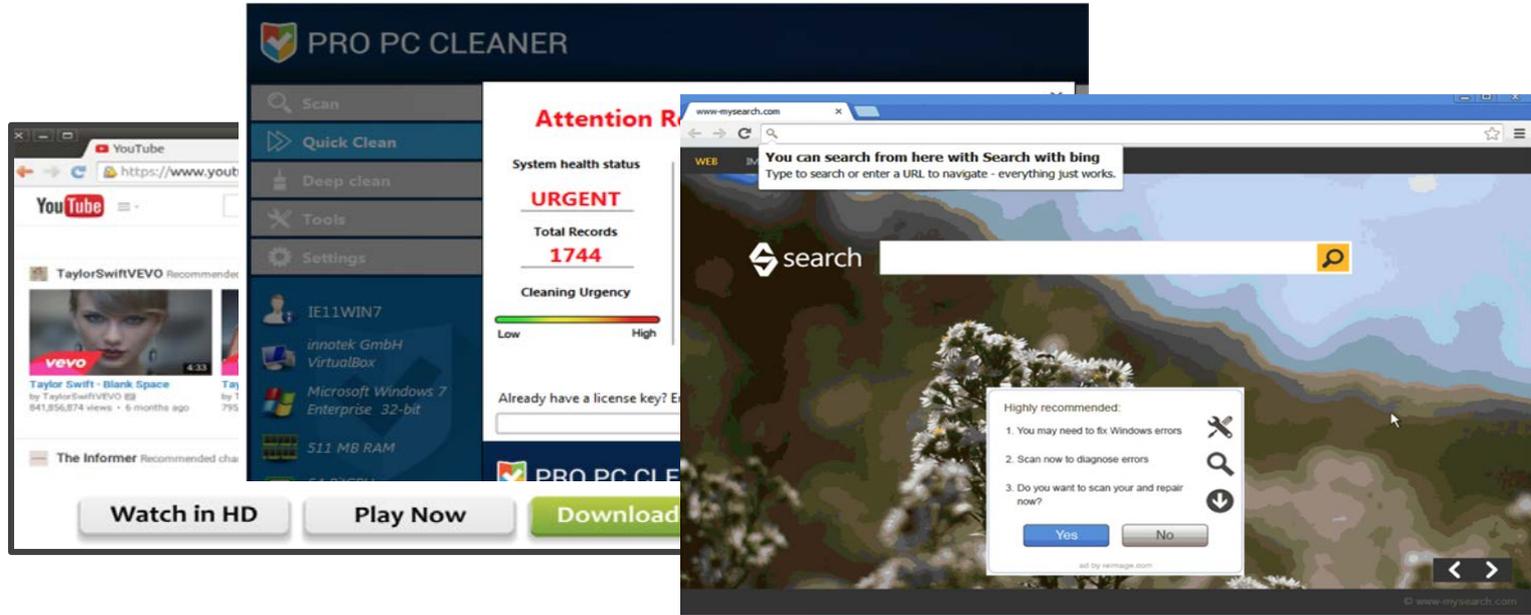
INVESTIGATING COMMERCIAL PAY-PER-INSTALL

Kurt Thomas, Juan A. Elices Crespo, Ryan Rasti, Jean-Michel Picod, Cait Phillips, Marc-André Decoste, Chris Sharp, Fabio Tirelo, Ali Tofigh, Marc-Antoine Courteau, Lucas Ballard, Robert Shield, Nav Jagpal, Moheeb Abu Rajab, Panos Mavrommatis, Niels Provos, Elie Bursztein, **Damon McCoy**



This research was funded by the National Science Foundation and Gifts from Google

Unwanted software



Millions of users with symptoms of unwanted software. How was it installed?

Commercial pay-per-install

Practice of bundling several additional applications.

The screenshot displays a multi-step installation wizard. The 'Setup Wizard' window shows 'Installation Options' with 'Install Options' selected. Below, it lists 'Optional Software: Search Quick Know' and provides a link to 'SEE BELOW FOR IMPORTANT INSTALLATION DISCLOSURES'. The 'Setup Setup' window prompts the user to click 'Next' and displays a scrollable text area containing a detailed privacy notice. The notice states that the software includes 'RelevantKnowledge' and that users' browsing and purchasing behavior will be monitored and used for market research. It also lists other bundled software: Plus-HD, Vuupp, GeekBuddy, OneSystemCare, GamesBot, Kickblaster, KNCTR, and AdBlockerPremium. The 'Accept' button is highlighted in red.

Setup Wizard
Setup Wizard: Installation Options
Welcome **Install Options**

Install Optional Software: Search Quick Know
SEE BELOW FOR IMPORTANT INSTALLATION DISCLOSURES
Install Search Quick Know to gain access to a new default search provider, homeStart Know's customized search experience in all compatible browsers. Also adds cool new shopping features, coupons, related search results, website ratings/reviews & exclusives.

Setup Setup
To continue installing your application, click on the Next button.

The download and installation process of this file is run by InstallPath Install Manager. By clicking the "Accept" or "Next" buttons below, or by continuing this InstallPath Install Manager installation, or otherwise using the Software, you agree to be bound by the terms of InstallPath Install Manager EULA (End User License agreement) located at <http://www.installpath.com/eula.html>, its Privacy Policy (<http://www.installpath.com/privacy.html>) and Terms of Service (<http://www.installpath.com/terms.html>). For more information, please see the Privacy Policy and Terms of Service.

Express Install (Recommended)
Start your installation and install Setup, Navision Global Data Remarketer, NoteUp, Network Manager, One Soft Per Day, Sushileads

Custom Install (Expert)

Privacy Policy
Help
Contact us

Close **Next >>**

Setup - Audio Convert Merge Free
Audio Convert Merge Free includes RelevantKnowledge
Active participants in RelevantKnowledge are recognized with a tree donation. Relevantknowledge.com/trees

In order to provide this free download, RelevantKnowledge software, provided by TMRG, Inc., a comScore, Inc. company, is included in this download. This software allows millions of participants in an online market research community to voice their opinions by allowing their online browsing and purchasing behavior to be monitored, collected, aggregated, and once anonymized, used to generate market reports which our clients use to understand Internet trends and customer and other market research purposes. The information which is monitored and collected includes, but is not limited to, the following: IP address, browser type, operating system, hardware, and application usage information about the computer on which the software is installed. We may use the information that we monitor, such as name, address, and household demographics; for example, we may combine this information with additional information from consumer data brokers and other sources to create a profile of you and your household. We make commercially viable efforts to protect personally identifiable information and to purge our databases of personally identifiable information when inadvertently collected. By clicking Accept you agree to the terms and conditions of the Privacy Statement, Terms of Service, and Patent Notice.

[Privacy Statement, EULA, and Patent Notice](#)

< Back **Next >** Cancel

Thank you for considering the installation of the following products. With the Express option you'll get the following apps for free: Plus-HD, Vuupp, GeekBuddy, OneSystemCare, GamesBot, Kickblaster, KNCTR & AdBlockerPremium.

By clicking "Accept" you confirm that you have read and agree to [Plus-HD, Vuupp, GeekBuddy, OneSystemCare, GamesBot, Kickblaster, KNCTR, AdBlockerPremium](#).

Accept

Deceptive promotions

The image is a collage of several screenshots illustrating deceptive software promotions:

- Windows 10 X64 6in1 v1511 ES**: A download page for Windows 10 with a large green **Download** button.
- Windows 7 Driver Optimizer**: A page for a Microsoft Gold Certified Partner software. It features a **Start Download** button and a **Download Free Video Player** button. The text includes: "System Information: Your machine is currently running: Windows 7. The Driver Update utility is compatible with your operating system." and "DriverSupport is a Five Star Rated Download with over 8 Million users worldwide. This free version scans and finds all Windows driver issues. The benefits of this software may include: Optimized Hardware Drivers (Printers, Scanners, Mouse, etc), Faster Windows Performance, Quicker Computer Startup Times, Fewer Hardware Error Messages, Increased Computer Stability & Performance."
- Your software may be out of date**: A notification from Open Software Updater.
- UPDATES RECOMMENDED!**: A dialog box with a red 'X' icon and buttons for **Cancel** and **OK**.
- You need to install the video player**: A black overlay with a green **DOWNLOAD FREE VIDEO PLAYER** button.

Users deceived into unintentionally installing unrelated software.

Our work

Year-long investigation into the marketplace of bundling:

Relationships with unwanted software

Deceptive promotional tools

Negative impact on users

Get the community on board to tackle unwanted software

1

BEHIND THE SCENES

Pay-per-install affiliate model

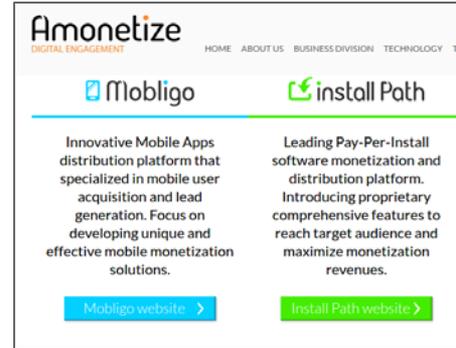


Advertisers: software developers willing to buy installs.

Pay-per-install affiliate model



Advertisers



PPI Network

PPI affiliate network: middle-man that create download manager.

Pay-per-install affiliate model



Advertisers

\$\$\$



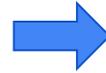
Amonetize
DIGITAL ENGAGEMENT

HOME ABOUT US BUSINESS DIVISION TECHNOLOGY TE

Innovative Mobile Apps distribution platform that specialized in mobile user acquisition and lead generation. Focus on developing unique and effective mobile monetization solutions.	Leading Pay-Per-Install software monetization and distribution platform. Introducing proprietary comprehensive features to reach target audience and maximize monetization revenues.
Mobligo website >	Install Path website >

PPI Network

\$\$



Windows 7 Driver Optimizer

Microsoft Video Player

facebook Chat Instant Messenger

Publishers

Publishers: popular software developers or websites that distribute bundles for a fee.

Pay-per-install affiliate model



Advertisers

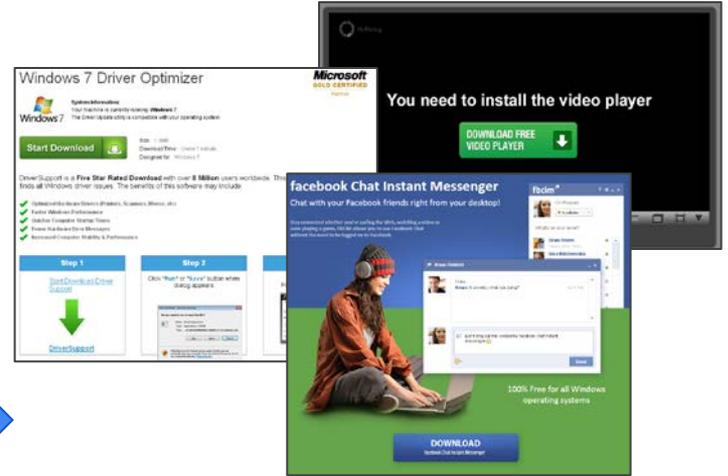


Amonetize
DIGITAL ENGAGEMENT

HOME ABOUT US BUSINESS DIVISION TECHNOLOGY TE

 Mobligo Innovative Mobile Apps distribution platform that specialized in mobile user acquisition and lead generation. Focus on developing unique and effective mobile monetization solutions. Mobligo website >	 Install Path Leading Pay-Per-Install software monetization and distribution platform. Introducing proprietary comprehensive features to reach target audience and maximize monetization revenues. Install Path website >
---	--

PPI Network



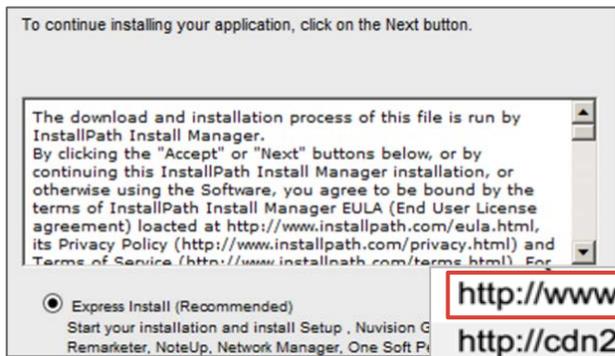
Publishers

Decentralized distribution can lend itself to abuse.

2

MONITORING PPI NETWORKS

Upon launching a PPI bundle...



C&C domain

- <http://www.myflowerdownload.com/index.php>
- <http://cdn2.lawfuldownload.com/9ee1efd2-b9b2-403>
- <http://cdn2.lawfuldownload.com/9ee1efd2-b9b2-403>
- <http://www.myflowerdownload.com/finalize.php>
- <http://cdn2.lawfuldownload.com/9ee1efd2-b9b2-403>
- <http://cdn2.lawfuldownload.com/9ee1efd2-b9b2-403>
- <http://www.myflowerdownload.com/thankyou.php>

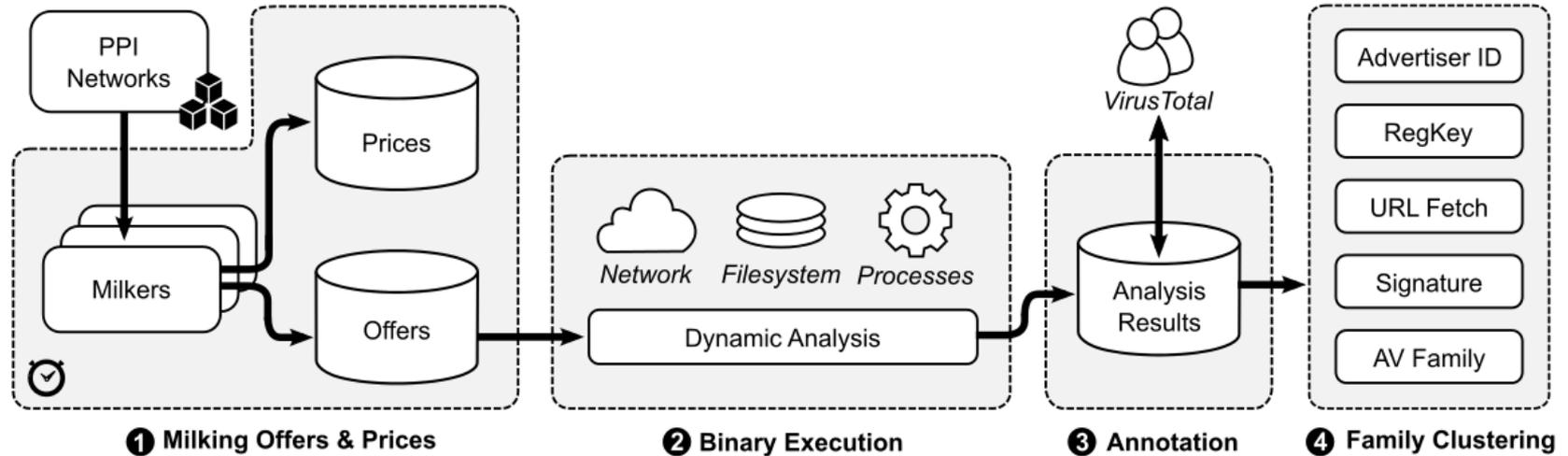
Fingerprint system & request offers

Report successful installs

Optional splash screen post-install



Analysis pipeline



Dataset

PPI Network	Milking Period	Offers	Unique
Outbrowse	Jan 8, 2015 -- Jan, 7, 2016	107,595	584
Amonetize	Jan 8, 2015 -- Jan, 7, 2016	231,327	356
InstallMonetizer	Jan 11, 2015 -- Jan, 7, 2016	30,349	137
OpenCandy	Jan 9, 2015 -- Jan, 7, 2016	77,581	134
Total	Jan 8, 2015 -- Jan, 7, 2016	446,852	1,211

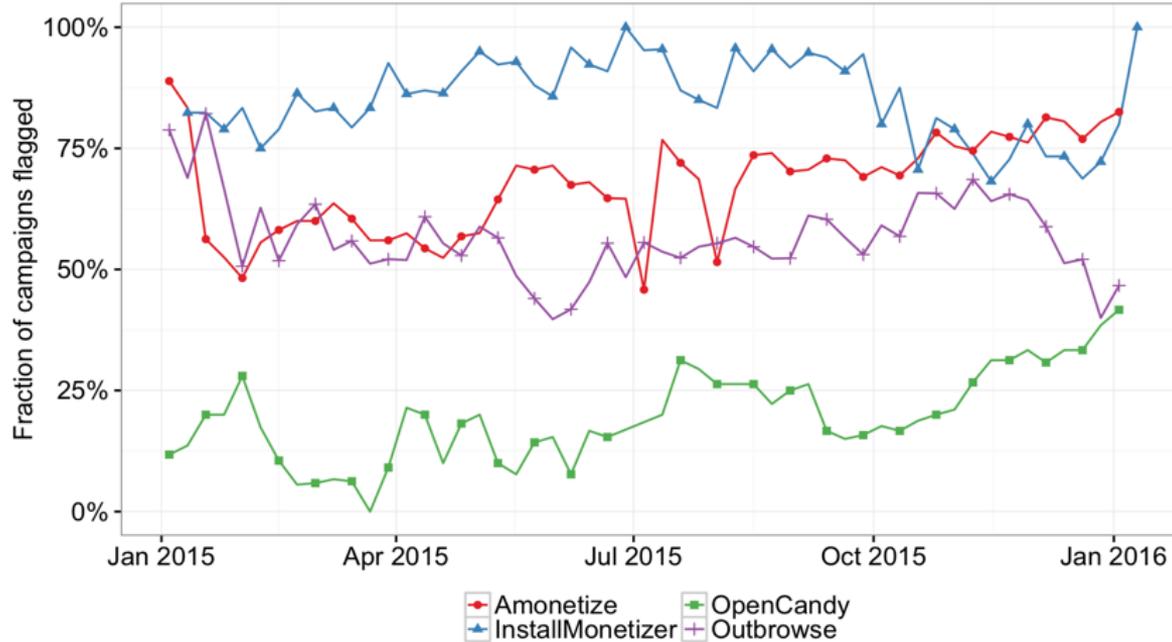
3

ANALYSIS

Most frequent advertisers

	Brand	PPI Networks	Days Active
Ad Injectors	<i>Wajam</i>	4	365
	<i>Vopackage</i>	3	365
	<i>Youtube Dwnldr</i>	3	365
	<i>Eorezo</i>	2	365
Browser Settings Hijackers	<i>Browsefox</i>	4	363
	<i>Conduit</i>	3	327
	<i>CouponMarvel</i>	1	300
	<i>Smartbar</i>	3	294
Cleanup Utilities	<i>Speedchecker</i>	2	365
	<i>Uniblue</i>	4	327
	<i>OptimizerPro</i>	4	302
	<i>Systweak</i>	3	249

VirusTotal labels



59% of weekly offers flagged by at least 1 AV

Anti-virus detection

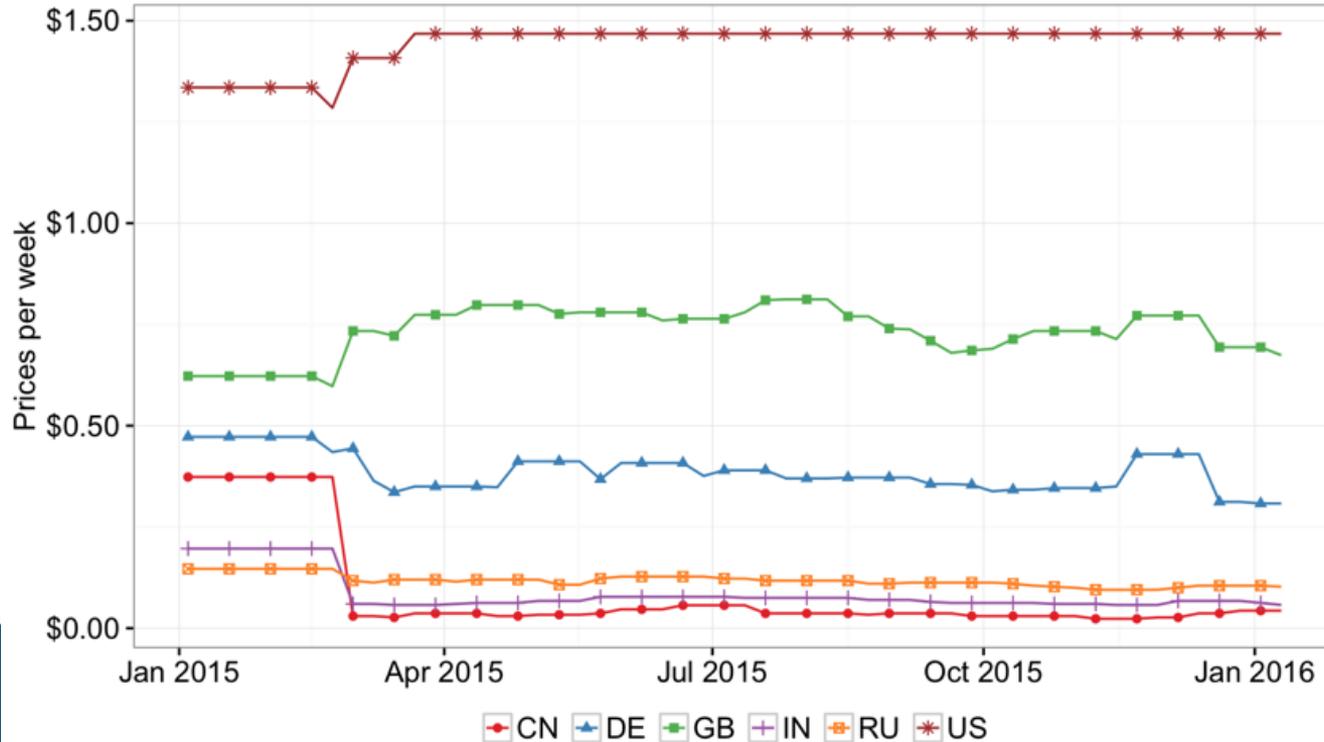
Advertiser-specified installation criteria avoids hostile AV:

```
(g_ami.CheckRegKey(g_hklmg_hk64, 'SOFTWARE\\\\\\Avast')!=0)
(g_ami.CheckRegKey(g_hkcu, 'SOFTWARE\\\\\\Avast')!=0)
(g_ami.CheckRegKey(g_hklmg_hk64, 'Software\\\\\\AVAST Software')!=0)
(g_ami.CheckRegKey(g_hkcu, 'Software\\\\\\AVAST Software')!=0)
(g_ami.CheckRegKey(g_hklmg_hk64, 'SOFTWARE\\\\\\Avira')!=0)
(g_ami.CheckRegKey(g_hklmg_hk64, 'SOFTWARE\\\\\\Classes\\\\\\avast')!=0)
(g_ami.CheckRegKey(g_hklmg_hk64, 'SOFTWARE\\\\\\ESET')!=0)
(g_ami.CheckRegKey(g_hklmg_hk64, 'AppEvents\\\\\\Schemes\\\\\\Apps\\\\\\Avast')!=0)
(g_ami.CheckRegKey(g_hklmg_hk64, 'SYSTEM\\\\\\CurrentControlSet\\\\\\Services\\\\\\avast! Antivirus ')!=0)
(g_ami.CheckRegKey(g_hklmg_hk64, 'SOFTWARE\\\\\\Microsoft\\\\\\Windows\\\\\\CurrentVersion\\\\\\Uninstall\\\\\\Avast')!=0)
(g_ami.CheckRegKey(g_hklmg_hk64, 'SOFTWARE\\\\\\{C1856559-BA5C-41B7-961C-677E89A2C490}')!=0)
(g_ami.CheckRegKey(g_hklmg_hk64, 'SOFTWARE\\\\\\{0D40F91C-41DE-4E06-8B14-ABCCF7A51495}')!=0)
(g_ami.CheckRegKey(g_hklmg_hk64, 'SOFTWARE\\\\\\{8B261394-6C7D-4CFC-A767-E02F34A60D8B}')!=0)
```

```
HKEY_LOCAL_MACHINE SOFTWARE\\\\\\OpenVPN
HKEY_LOCAL_MACHINE SOFTWARE\\\\\\VMware,*Inc.
HKEY_LOCAL_MACHINE SOFTWARE\\\\\\Oracle\\\\\\VirtualBox|
```

20% of advertisers use some AV/VM detection

Price per install



Price ranges
\$0.10–\$1.50

4

USER IMPACT

Unwanted software warnings



The site ahead contains harmful programs

Attackers on [www.dominionenergy.com](#) might attempt to trick you into installing programs that harm your browsing experience (for example, by changing your homepage or showing extra ads on sites you visit).

Automatically report details of possible security incidents to Google. [Privacy policy](#)

[Details](#)

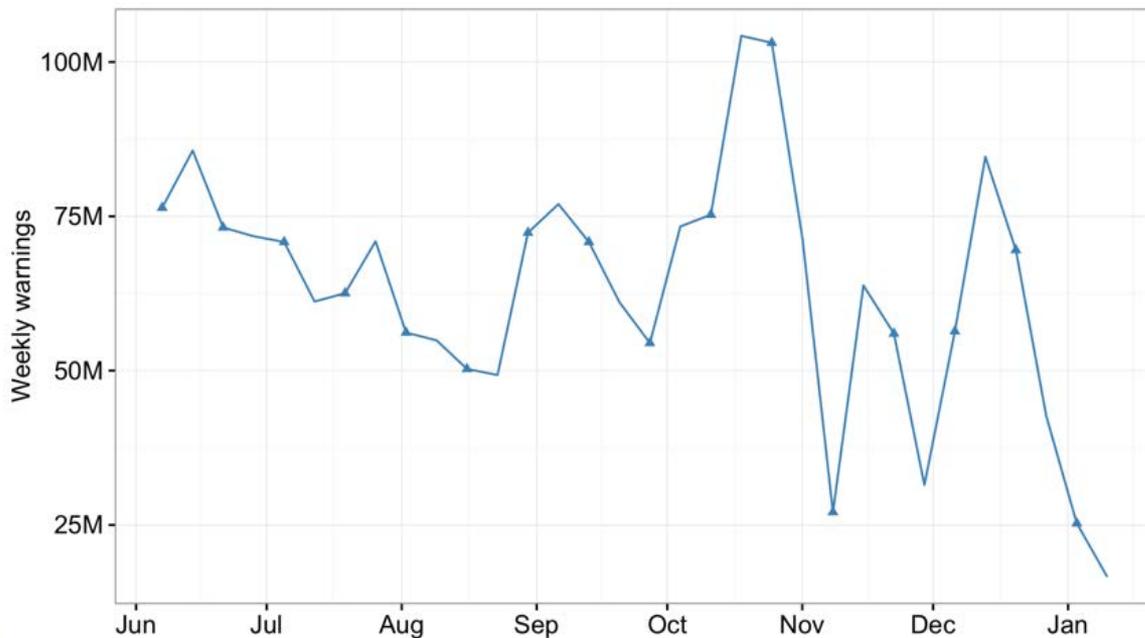


pua.exe may harm your browsing experience, so Chrome has blocked it.

Dismiss



Weekly user warnings



*60M warnings
every week*

5

DECEPTIVE DISTRIBUTION

Promotional tools

PERINSTALLCASH NEWS STATISTICS MANAGE PROMOTOOLS PAYMENTS HELP LOG OUT

Home / Promo tools

Promo tools

Attention! Never save any exe-files to your server! Outdated distributives may cause

Show All Movie traffic Download traffic Youtube traffic MP3 traffic S

DIRECT LINK

Software



NEW! Basic direct download link for common cases. Place it on your site and see how profit grows.

» How to setup

LINK LOCKER

Software



Lock any URL with our Link Locker and get paid when user installs the software to access the link.

» How to setup

uTorrent Download #2 (add parameters fn=File_to_download.zip size=sizeinMB)

Copy this link and use on your website:

[preview](#)

[View banners \(4\)](#)



Java Update Download (add parametr auto=1 for auto download exe)

Copy this link and use on your website:

[preview](#)



Java Update Error (add parametr auto=1 for auto download exe)

Copy this link and use on your website:

[preview](#)



Domain cycling

07

New domains New

IMPORTANT!!!

Jan

We replaced some blocked promo domains with new ones. Please change it at your side as soon as possible, using of old domains can lead to profit loss.

Old domain => New domain:

letshareus.com => letshare.club

downloadsoundcloud.net => downloadsoundcloud.xyz

fbmessenger.net => fbchat.xyz

mp3gino.com => ginoplayer.xyz (also dynamic banners are now on blocks.ginoplayer.xyz)

loadvids.net => loadvids.xyz

saveclip.net => saveclip.xyz

wallpapermanager.net => wallpaperman.xyz

Also, note that our main direct download domain now is download5-cdn.com, so if you still use download4-cdn.com or download3-cdn.com - replace it as soon as possible.

*Distribution sites
cycle every 1-7
hours*

Safe Browsing evasion



Takeaways

Unwanted software massive commercial ecosystem:

Tens of millions of users affected

Pay-per-install primary distribution vector

Misaligned incentives for advertisers, publishers

Killed by Proxy: Analyzing Client-end TLS Interception Software

Xavier de Carné de Carnavalet and Mohammad Mannan
Concordia University, Canada

Funding support: **Vanier CGS, NSERC, and OPC**
Original publication: **NDSS 2016**

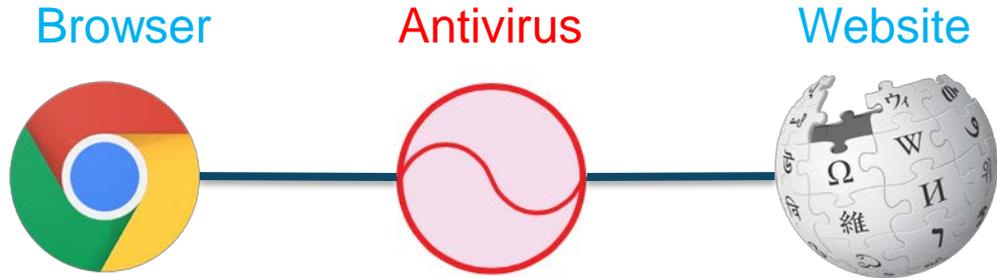
HTTPS usage

- Secures client-server connection
- > half the websites now support HTTPS



Antivirus vs. HTTPS

- Both help secure your data/online experience
- AVs also want to guard against web malware
- But malware may come via HTTPS



Client-end TLS interception

1. **Ad**-related products (SuperFish/PrivDog/Komodora)
 - inject/replace ads
2. **Antivirus** products
 - eliminate drive-by downloads, malicious scripts
3. **Parental** control applications
 - block access to unwanted websites, hide swear words

Wanted vs. unwanted interception

- Unwanted adware can/should be removed
- But AVs and parental control apps are
 - “wanted”
 - “strongly recommended” or “required”

Our targets

- 14 security products in Windows
 - March and August 2015
- All but one significantly downgrade TLS security



Implications

- Attacker must be an active **Man-in-the-Middle**
 - Anywhere between a user and website
 - Target all users of a product vs. selective users
 - No admin privilege is needed
- **Can impersonate a server**
- **Can extract secrets** e.g., authentication cookies
- **Design flaws** – not software bugs

Federal Trade Commission x

← → ↻ <https://www.ftc.gov>

FEDERAL EPIC FAIL
PROTECTING AMERICA'S

ABOUT THE FTC NEWS & EVENTS

Security Overview

Overview

Main Origin

https://www

This page is secure

Valid Certificate

The connection

View certificate

Secure Connection

The connection protocol (TLS 1.2) uses strong cipher (AES256-GCM-SHA384)

Secure Resources

All resources on this page are secure

Certificate

General Details Certification Path

Show: <All>

Field	Value
Issuer	www.contentwatch.com, ContentWa...
Valid from	Monday, January 2, 2017 3:33:05 PM
Valid to	Tuesday, January 2, 2018 3:33:05 PM
Subject	xmas-gifts@ftc.gov, www.ftc.gov, C...
Public key	RSA (1024 Bits)
Public key parameters	05 00
Thumbprint algorithm	sha1
Thumbprint	2c c5 c9 69 c4 65 ae 54 6b 4b 35 13 c...

E = xmas-gifts@ftc.gov
CN = www.ftc.gov
OU = CHRISTMAS DEPARTMENT
O = COCA-COLA
L = North Pole
S = -
C = CA

Edit Properties... Copy to File...

Our test framework

Hybrid test framework: adapt existing + custom tests

1. Private key protection
2. Certificate validation
3. Cipher suites & protocols
4. Transparency

Root certificate and private key

- **Pre-generated** certificates (2/14)
- Proxies **accept own certificates** (12*/12)
- **User-readable** private keys (9/14)
- Root cert. not removed after **uninstallation** (8/14)
- Certificates are valid, on average, for **10 years**

Site certificate validation

- **No validation** (3/12)
- Improper signature verification (1/12)
- Accept weak primitives: **MD5** (9/12), **RSA 512** (7/12)
- No revocation check (9/12)
- Custom CA store (3/12): **DigiNotar+CNNIC**; Mozilla Trusted CAs from 2009; One **RSA 512 root CA**

Protocol, cipher suites and attacks

- **SSL 3.0** support (6/12), no support for TLS 1.1+ (6/12)
- Weak cipher suites: **RC4 and MD5** (10/12)
- Proxies **vulnerable to known attacks**: Insecure Renegotiation (1), BEAST (7), CRIME (1), FREAK (5), Logjam (3)

Proxy transparency

- **Virtual upgrade** of TLS version as seen by the client (7/12)
 - SSL 3.0 → TLS 1.0 or 1.2
 - TLS 1.0 → TLS 1.2
- Cipher-suites are **never transparent**, client's choice ignored
- **EV certificates** filtered, replaced by DV (11/12)

Summary results

	Certificate generation time	Reject own root certificate	Removal during uninstallation	Validity (years)	Key protection	Access right
Avast	Installation	×	✓	10	OS API	Admin
AVG	Installation	✓*	✓	10	Obfuscation	Unknown
BitDefender	Installation	×	✓	10	Hardcoded pwd	User
BullGuard AV	Installation	—	×	10	Hardcoded pwd	User
BullGuard IS	Installation	✓	×	10	Hardcoded pwd	User
CYBERsitter	Pre-generated*	×	×	20	Plaintext	User
Dr. Web	Installation	×	×	1	OS API	Admin
ESET	Installation*	×	×	10	OS API	Admin
G DATA	Installation	×	✓	10	Obf. encryption	User
Kaspersky	Installation	×	×	10	Plaintext	User
KinderGate	Installation	×	×	5	Plaintext	User
Net Nanny	Installation	×	✓	10	Modified SQLCipher	User
PC Pandora	Pre-generated	×	✓	10	OS API	Admin
ZoneAlarm	Installation	—	×	10	Plaintext	User

Recommendations

- Use TLS "key-logging"
- **Private keys**: Use OS-provided storage APIs
- **Certificate validation**: Rely on an updated TLS library, communicate errors to users
- **Transparency**: Respect client's choice
- **Browsers/servers**: More pro-active, warn users when proxied

Takeaways...

1. “More security” (software) may be bad users
 - increased attack surface
2. How to hold AVs responsible?
3. Periodic monitoring – needs regulatory help?

Madiba Security Research Group
<https://madiba.encs.concordia.ca>

Discussion of Session 5

Presenters:

- **Amin Kharraz**, Northeastern University
- **Damon McCoy**, New York University
- **Mohammad Mannan**, Concordia University, Canada

Moderator:

- **Mark Eichorn**, Federal Trade Commission

Wrap-Up Panel

Panelists:

- **Howard Beales**, George Washington University
- **Deirdre Mulligan**, University of California, Berkeley
- **Andrew Stivers**, Federal Trade Commission

Moderator:

- **Jessica L. Rich**, Federal Trade Commission

THANKS!

A dark blue silhouette graphic at the bottom left of the slide, featuring a large cloud-like shape on the left and several interlocking gears of various sizes extending to the right.

PRIVACYCON