



The PC Security Channel

Stay Informed. Stay Secure.



Context Aware Detection

The future of Cybersecurity?

Rohit Satpathy @leotpsc | Founder, The PC Security Channel

About



The PC Security Channel

Stay Informed. Stay Secure.

“Leo from The PC Security Channel”



About





The PC Security Channel

Stay Informed. Stay Secure.

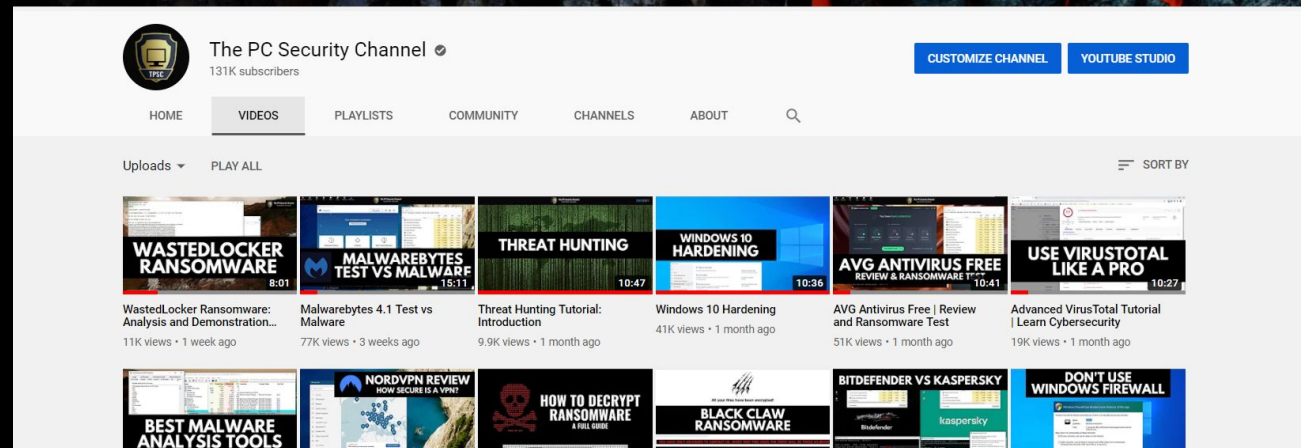
CYBERSECURITY FOR EVERYONE

STAY INFORMED. STAY SECURE

Official Website  

130,000
Subscribers

15 Million
Views



The screenshot shows the YouTube channel page for 'The PC Security Channel'. The channel has 131K subscribers. The page layout includes a header with the channel name and subscriber count, followed by navigation tabs: HOME, VIDEOS, PLAYLISTS, COMMUNITY, CHANNELS, and ABOUT. Below the navigation is a section for 'Uploads' with a 'PLAY ALL' button. The main content area displays a grid of video thumbnails. Each thumbnail includes a title, a duration, and a view count with the time it was posted. The videos are as follows:

Video Title	Duration	Views	Posted
WastedLocker Ransomware: Analysis and Demonstration...	8:01	11K	1 week ago
Malwarebytes 4.1 Test vs Malware	15:11	77K	3 weeks ago
Threat Hunting Tutorial: Introduction	10:47	9.9K	1 month ago
Windows 10 Hardening	10:36	41K	1 month ago
AVG Antivirus Free Review and Ransomware Test	10:41	51K	1 month ago
Advanced VirusTotal Tutorial Learn Cybersecurity	10:27	19K	1 month ago
BEST MALWARE ANALYSIS TOOLS			
NORDVPN REVIEW: HOW SECURE IS A VPN?			
HOW TO DECRYPT RANSOMWARE: A FULL GUIDE			
BLACK CLAW RANSOMWARE			
BITDEFENDER VS KASPERSKY			
DON'T USE WINDOWS FIREWALL			

Prelude



The PC Security Channel

Stay Informed. Stay Secure.

“In the information society, nobody thinks. We expected to banish paper, but we actually banished thought” - Michael Crichton

Scientist – “My findings are pointless when taken out of context”

Correction published by media – Scientist claims “findings are pointless”

Modern cyber threats



The PC Security Channel

Stay Informed. Stay Secure.

- Fileless malware
- Zero-day attacks
- Hacked systems
- Data breaches
- Stolen credentials
- APTs

In most cases detection technology is powerless to stop these threats.

Meanwhile...

A simple script for a popup that says “Happy Birthday, Dad” is detected by 25 engines on VirusTotal.

Modern detection parameters



The PC Security Channel

Stay Informed. Stay Secure.

- Digital Signatures
- Import DLLs and Functions
- Packing Techniques
- Strings related to the use of certain calls
- File entropy
- Section ranges
- TLS features

Q: Why do any of these indicate that a file is malicious?

A: They just do!

Cause that's what we see in the malware.

Proactive or reactive?



The PC Security Channel

Stay Informed. Stay Secure.

Malware **performs** behaviour
Analysts **research** malware
Detection **strategy** created
Product **detects** behaviour

Eventually the list of malicious behaviours expands to include almost all possible operations, and users complain about FPs.

What to do now?

Whitelist all the safe files.

Back to square one.

Back to first principles



The PC Security Channel

Stay Informed. Stay Secure.

“I tend to approach things from a physics framework, and physics teaches you to reason from first principles rather than by analogy” - Elon Musk

Malware “Malicious Software”

Malicious /mə'ɪʃəs/ Adjective
characterized by malice; intending or intended to do harm.

“Intent”

What is malicious behaviour?



The PC Security Channel

Stay Informed. Stay Secure.

Transferring data to a server isn't malicious

Infostealers are

Cryptomining isn't malicious

Silent cryptominers are

File encryption isn't malicious

Ransomware is

What makes these behaviours malicious is context.



The PC Security Channel

Stay Informed. Stay Secure.



Mal X Project

Cybersecurity testing, malware analysis and beyond.

How Mal X works



The PC Security Channel

Stay Informed. Stay Secure.

Mal X launches **suspected malware**

Gathers **PE Metadata** for **Static Analysis**

Performs **Dynamic Analysis** based on program behaviour

Tests **system cybersecurity** and **classifies malware**

Experiment: Classify files into PUPs, Malware and most importantly, **Irrelevant data**

How?

How Mal X works



The PC Security Channel

Stay Informed. Stay Secure.

Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-4B3FDQ2\Leo]

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	Virtual
svchost.exe		1,596 K	2,516 K	6124	Host Process for Windows S...	Microsoft Corporation	0/68
svchost.exe		6,572 K	3,852 K	3496	Host Process for Windows S...	Microsoft Corporation	0/68
svchost.exe		43,316 K	37,756 K	6380	Host Process for Windows S...	Microsoft Corporation	0/68
svchost.exe		2,588 K	11,732 K	10000	Host Process for Windows S...	Microsoft Corporation	0/68
PSEXESVC.exe		1,620 K	6,304 K	10008	PsExec Service	Sysinternals	1/70
powershell.exe		64,740 K	74,784 K	8700	Windows PowerShell	Microsoft Corporation	0/63
conhost.exe	0.64	10,344 K	22,948 K	668	Console Window Host	Microsoft Corporation	0/70
python.exe	10.06	18,328 K	32,164 K	6332	Python	Python Software Foundation	0/71
Test.exe		3,196 K	7,528 K	6304	Setup For Warcraft III: Refor...		21/70
Test.tmp	0.47	22,176 K	30,976 K	892	Setup/Uninstall		0/72
svchost.exe		2,732 K	8,828 K	3268	Host Process for Windows S...	Microsoft Corporation	0/68
svchost.exe		1,736 K	6,932 K	4608	Host Process for Windows S...	Microsoft Corporation	0/68
svchost.exe		5,324 K	16,716 K	6568	Host Process for Windows S...	Microsoft Corporation	0/68
svchost.exe		1,460 K	5,820 K	3704	Host Process for Windows S...	Microsoft Corporation	0/68
svchost.exe		25,648 K	36,432 K	5672	Host Process for Windows S...	Microsoft Corporation	0/68
svchost.exe		4,040 K	13,876 K	6716	Host Process for Windows S...	Microsoft Corporation	0/68
svchost.exe		1,300 K	5,516 K	1912	Host Process for Windows S...	Microsoft Corporation	0/68
svchost.exe		7,664 K	13,052 K	736	Local Security Authority Proc...	Microsoft Corporation	0/68
fontdrvhost.exe		1,264 K	1,352 K	896	Usermode Font Driver Host	Microsoft Corporation	0/72
csrss.exe	0.14	1,796 K	11,632 K	580	Client Server Runtime Process	Microsoft Corporation	0/68
winlogon.exe		2,876 K	4,152 K	672	Windows Logon Application	Microsoft Corporation	0/70
fontdrvhost.exe		3,940 K	7,624 K	904	Usermode Font Driver Host	Microsoft Corporation	0/72
dmv.exe	0.44	110,460 K	134,624 K	400	Desktop Window Manager	Microsoft Corporation	0/70
explorer.exe	0.65	60,272 K	101,612 K	9556	Windows Explorer	Microsoft Corporation	0/68
vm3dservice.exe		1,412 K	2,240 K	8148			0/72
vmtoolsd.exe	0.03	28,120 K	40,080 K	8176	VMware Tools Core Service	VMware, Inc.	0/73
process64.exe	0.80	26,312 K	49,904 K	9324	Sysinternals Process Explorer	Sysinternals - www.sysinter...	1/69

CPU Usage: 14.05% Commit Charge: 35.60% Processes: 145 Physical Usage: 44.39%

Administrator: C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe

```
New File handle: C:\Windows\Fonts\StaticCache.dat
New File handle: C:\Windows\WinSxS\x86_microsoft.windows.c...controls.resources_6595b64144ccf...
ldf_6.0.18362.535_en-gb_3cf377e55909af4f\comctl32.dll.mui
New File handle: C:\Windows\SystemResources\shell32.dll.mun
Title: Warcraft III: Reforged - Type: None - Path: C:\Windows\Temp\is-lVCET.tmp\Test.tmp
Title: Warcraft III: Reforged - Type: None - Path: C:\Windows\Temp\is-lVCET.tmp\Test.tmp
Title: - Type: None - Path: C:\Windows\explorer.exe
```

What makes a file, malware?



The PC Security Channel

Stay Informed. Stay Secure.

Does it perform actions that result in a detrimental outcome for the user?

Does it perform actions without the user's consent?

Does it hide itself partly or completely from the user?

User Interaction



Program

How Mal X works



The PC Security Channel

Stay Informed. Stay Secure.

Case: Application is a cryptominer

Is it malware?

How does it interact with the user?

- Windows presented
- Input from user before mining begins
- Persistence (hidden installations)
- Is it easy to remove?

Everything hinges on **program-user interaction**

Undervalued Parameters



The PC Security Channel

Stay Informed. Stay Secure.

Screenshots: What is happening on screen?

Windows Open: What does the application present to the user?

Window Titles: What does the application say is being presented to the user?

User Input: Does the user interact with the application?

File Handles: What other files are being accessed or written by the applications?

Observations



The PC Security Channel

Stay Informed. Stay Secure.

True Trojans are quite uncommon

Most malicious applications perform their actions silently

- > New Application or Process appears
 - > Does not notify or interact with the user
 - > Performs sensitive operations without permission or notification
 - > **Detection**

All that user data



The PC Security Channel

Stay Informed. Stay Secure.

“With great power comes great responsibility” - Voltaire

Telemetry to Telemarketing

No, thank you.

Attention to vulnerabilities

Trust is the most important feature for a cybersecurity product.

Credits



The PC Security Channel

Stay Informed. Stay Secure.

TPSC



DISCORD

@floriegl for development

EMSISOFT



Questions?



The PC Security Channel

Stay Informed. Stay Secure.

Thank you.

Feel free to reach out.

Email: leo@tpsc.tech

Website: tpsc.tech

Twitter: [@leotpsc](https://twitter.com/leotpsc)

YouTube: youtube.com/thepcsecuritychannel