peerlyst®


# 32 Influential Malware Research Professionals

## 32 malware researchers you should know

Compiled by Chiheb Chebbi

## 32 Influential Malware Analysis professionals

(In no specific order)

- Hasherezade
- Monnappa K A
- Chi-en Shen (Ashley Shen)
- Jan Sirmer
- Luca Nagy
- Abhinav Singh
- Thaís Moreira Hamasak
- Alexander Sevtsov
- Lukas Stefanko
- Ali Ahangari
- Alexandre Borges
- Karsten Hahn
- Kenneth Bechtel
- Jimmy Wylie
- Thomas Chopitea
- Douglas McKee
- Mark Lechtik
- Fumik0_
- Silas Cutler
- Marcus Hutchins
- William Meyers
- Michael Gillespie
- Brian Baskin
- Seongsu Park
- Luca Mella
- Clay Dunnavant
- Pollo290987
- Albert Zsigovits
- Vitali Kremez
- Jaromir Horejsi
- Ruben shotgunner101
- That_malware_guy

Compiled by: Chiheb Chebbi

# Hasherezade

@hasherezade

Aleksandra Doniec (@hasherezade) is passionate about IT since early teenage years. From that time she collected a wide range of experience – working as a scientific researcher, programmer, pentester and analyst. Currently works as a malware intelligence analyst for Malwarebytes, sharing knowledge about the current threats it in technical blog posts, as well as on a private YouTube channel. She is an author and active maintainer of several free and open-source tools, mostly related to malware analysis, i.e. PE-bear, PE-sieve.

# Monnappa K A

Monnappa K A works for Cisco Systems as an information security investigator focusing on threat intelligence and investigation of advanced cyber attacks. He is the author of the best selling book "Learning Malware Analysis".He is the review board member for Black Hat Asia, Black Hat USA and Black Hat Europe. He is the creator of Limon Linux sandbox and winner of Volatility plugin contest 2016. He is the co-founder of the cybersecurity research community "Cysinfo" (https://www.cysinfo.com). He has presented at various security conferences including Black Hat, FIRST, SEC-T, 4SICS-SCADA/ICS summit, DSCI and Cysinfo on various topics which include memory forensics, malware analysis, reverse engineering, and rootkit analysis. He has conducted training sessions at Black Hat, BruCON, HITB, FIRST, SEC-T and OPCDE cyber security conferences. He has also authored various articles in eForensics and Hakin9 magazines. He regularly conducts training titled "A Practical Approach to Malware Analysis & Memory Forensics" around the world including Black Hat USA, Black Hat Asia, Black Hat Europe, HITB and BruCON security conferences.

Monnappa K A

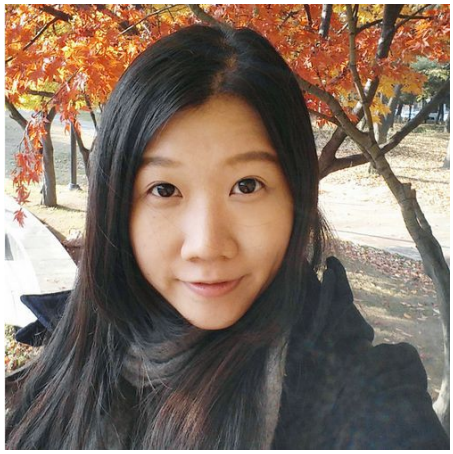
Monnappa K A

@monnappa22

MonnappaKA

https://cysinfo.com

# Chi-en Shen (Ashley Shen)



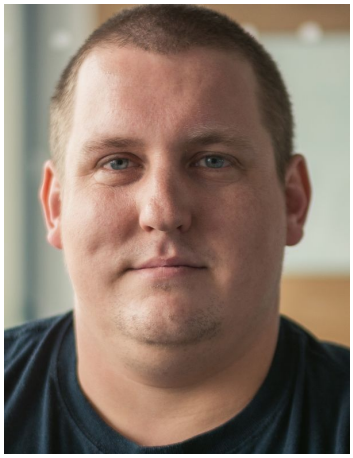
Chi-en Shen (Ashley)

@ashley_shen_920

Chi-en Shen (Ashley) is a researcher from Taiwan who focus on malware and threat intelligence research. Chi-en is passionate about hacking techniques since early teenage years. She started her career five years ago as a co-founder and cyber threat analyst in Team T5, where she did malware research and campaign tracking to reveals several targeted attack activities. Chi-en is currently the senior researcher for FireEye, where she works on threat hunting and researching targeted attacks against Asia Pacific. For sharing knowledge, Chi-en frequently speaks in international security conferences, including Black Hat, FIRST, HITB GSEC, Confidence, CODE BLUE, SecTor, Troopers, HITCON, RESET, Cyber Defense Summit...etc.

For supporting women in InfoSec, Chi-en co-founded "HITCON GIRLS" – the first security community for women in Taiwan in 2014. She organized workshops, study groups and events to provide more opportunities for women to learn about cyber security and advocate a more welcoming culture in the industry. In 2018, she also helped to hold a "Women in Security" event in Black Hat Asia. Chi-en is also invited to serve in multiple review boards, including Black Hat Asia, Blue Hat Shanghai and Hack in the Box conferences.

# Jan Sirmer



I work as a Malware Analysis Team Lead at Avast Software. My main specialization is analyzing malicious Java threats, Android applications and exploits, macro viruses, web based malware and other non-executable malware. During the course of my career, I have authored blog posts about phishing threats, malicious web exploits and Android threats. In the past, I have successfully presented my research at various conferences such as AVAR, CARO, FIRST, Virus Bulletin, RSAC APJ and WebExpo.

Jan Sirmer

Jan Sirmer

@sirmer_jan

# Luca Nagy

The first time I came across programming languages was during high school and it was love at first sight. Our romance continued at university and I decided to dedicate myself to programming. While there, I also developed an interest in IT security and it was a huge dilemma to choose which direction to take my studies in.

For this reason, I started a CEH (Certified Ethical Hacker) course where we studied several techniques
and tools to find and exploit weaknesses in various systems. This required prior experience but also creativity to solve new problems. The combination was really appealing, and it helped me to reach the decision to take the IT security route in my career.
During an internship at Telekom, I was working with intrusion detection/prevention systems (IDS/IPS) and became acquainted with malware. I decided to dig deeper, and in my thesis, I introduced a malware analysis procedure through a ransomware analysis. I became passionate about malware analysis and have been ever since.
Now at Sophos, I spend my time reverse engineering emerging threats and creating detections against
them, but I am highly interested in memory forensic.

Luca Nagy

Luca Nagy

.

# Abhinav Singh


Abhinav Singh is an information security researcher currently working for Netskope, Inc. He is the author of Metasploit Penetration Testing Cookbook (first, second & third editions) and Instant Wireshark Starter, by Packt which has sold over 10,000 copies worldwide. His books have also featured as a reference material and learning resources in top universities around the world. He is an active contributor to the security community in the form of paper publications, articles, blogs, and mentorship. His work has been quoted in several security publications and digital portals. He is a frequent speaker at eminent international conferences like Black Hat, RSA, Defcon etc. He is also a review board member of RSA and ISSA. His areas of expertise include malware research, reverse engineering, enterprise security, forensics, and cloud security.

Abhinav Singh

Abhinav Singh

@abhinavbom

# Thaís Moreira Hamasak

Thaís Moreira Hamasak is a security researcher at Intel STORM (STrategic Offensive Research & Mitigations Team). Previous to that, she worked as a malware researcher @ F-Secure, with focus on static analysis, reverse engineering and logical programming. Thaís started her career within the anti-virus industry working on data and malware analysis, where she developed her knowledge on threat protection systems. She won the "best rookie speaker" award from BSides London for her very first talk about "Using SMT solvers to deobfuscate malware binaries". Recent research topics include binary deobfuscation, generic unpacking and static analysis automation. She is an active member of the Düsseldorf Hackerspace, where she also leads the groups for Reverse Engineering and x86 Assembly. In her free time, you can find Thaís building tools, cooking or climbing somewhere offline.

@barbieauglend

# Alexander Sevtsov

Alexander Sevtsov, Malware Reverse Engineer at Lastline. I started my career path more than 8 years ago (June 2011) at Kaspersky mostly working on improving detection against different web-threats (drive-by download attacks and exploit kits). Later on, I joined Avira to solve clustering and classification problems of Potentially Unwanted Applications (a.k.a PUA) based on behavior analysis. Currently I am working as a reverse engineer at Lastline focusing on dissecting evasive malware and sandbox improvements. My research interests are modern virtualization and emulation technologies, and deep document analysis.

Alexander Sevtsov

@alexsevtsov

# Lukas Stefanko

Lukas Stefanko is an experienced malware researcher with a strong engineering background and a well-demonstrated focus on Android and mobile security. Lukas in the past couple of years has made major strides towards heightening public awareness (globally) around Android threats and security.

Lukas Stefanko

@LukasStefanko

# Ali Ahangari

Ali Ahangari is a security analyst expert and founder of Hypersec blog, the first threat hunting blog in Iran. he has a demonstrated history of working in the IT industry, skilled in Threat Analysis/Hunting, Security Operation Center(SOC), Penetration Testing, and Linux. Strong information technology professional with a Master's Degree focused in Computer Software Engineering.

Ali Ahangari

Ali Ahangari

# Alexandre Borges

Alexandre Borges is a Security Researcher, who has been daily working on Reverse Engineering, Android/MacOS/iOS reversing and Digital Forensic Analysis for many years. Furthermore, Alexandre is the creator and maintainer of Malwoverview triage tool: https://github.com/alexandreborges/malwoverview.

Alexandre has spoken in several conferences such as DEF CON USA (2019 and 2018), DEF CON CHINA (2019), NO HAT Conference 2019, (Bergamo/Italy), DC2711 Conference (Johannesburg), CONFidence Conference 2019 (Poland), HITB 2019 Amsterdam, H2HC Conference (2015/2016), BSIDES Sao Paulo (2019/2018/2017/2016), DevOpsDays BH (Belo Horizonte/Brazil) and BHACK Conference (2019 and 2018).

Finally, it is a referee of Digital Investigation:The International Journal of Digital Forensics & Incident Response (https://www.journals.elsevier.com/digital-investigation/editorial-board)

Alexandre Borges

Alexandre Borges

@ale_sp_brazil

Malwoverview

# Karsten Hahn

@struppigel

Karsten works as Malware Analyst at G DATA CyberDefense AG. He is also part of the Anti-Ransomware group behind ID Ransomware (https://id-ransomware.malwarehunterteam.com), who have helped individuals and organizations to retrieve their ransomware encrypted files for free via identification and decryption tools. Besides ransomware he is also very interested in file format anomalies, especially in Portable Executable files. In his free time he creates malware tutorial videos for his MalwareAnalysisForHedgehogs channel on YouTube.

# Kenneth Bechtel

Kenneth (Ken) Bechtel first discovered malware in August of 1988 when he read a paper on the subject while serving in the US Army. Upon reading the paper he understood the impact of the matter and started researching the subject and how to defend against malicious code and attacks.

Ken's expertise in Anti-virus has been influential in founding organizations such as the Anti-Virus Information Exchange Network (AVIEN), which brings corporate researchers and administrators together to share information on malware threats; and Team Anti-Virus, which serves as an umbrella organization for like-minded independent anti-virus researchers. Ken also co-authored the AVIEN Malware Defense Guide.

An established IT industry professional, Ken has spoken at well-known conferences such as Virus Bulletin and has appeared on more than 30 local Television news shows. His work has been published in trade magazines and specialized web sites such as Security Focus. Ken was also invited to join the WildList Organization as a reporter in 1998.

With more than 29 years of IT experience, Ken's ideas have been widely adopted in the corporate arena and are respected in the security and malware research circles. He is a strong advocate for education, maintaining that education remains one of the best defenses in the fight against malware.

Kenneth Bechtel

Kenneth Bechtel

# Jimmy Wylie


Jimmy Wylie is a Senior Adversary Hunter at Dragos who spends his days (and nights) searching for and tearing apart threats to critical infrastructure. Starting as a hobbyist in 2009, he has over 10 years experience with reverse engineering and malware analysis. As a professional in the U.S. Intelligence Community, he utilized a wide range of skills against national level adversaries, including network analysis, dead disk and memory forensics, in-depth malware analysis, and software development supporting the detection, analysis and classification of malware in a variety of programming languages. Before joining Dragos, he was a course developer and instructor at Focal Point Data Risk, teaching a wide range of malware analysis techniques starting with beginner behavioral analysis and ending with kernel driver analysis.

Jimmy Wylie

Jimmy Wylie

# Thomas Chopitea

Thomas Chopitea is a forensics investigator and engineer at Google (he used to do work in the CERT of a big financial institution, but he's fine now). When he's not writing code and hunting down bad guys, he enjoys poking malware with a long stick and reading up on threat intelligence processes. His long-term professional goal is to automate himself out of a job.

@tomchop_

# Douglas McKee

Douglas McKee is a Senior Security Researcher within the McAfee Advanced Threat Research team. In this role, he is focused on finding new vulnerabilities in both software and hardware and mentoring incoming threat researchers.

Douglas began his career working for the U.S. Department of Defense where he gained wide exposure to the security industry through his work on vulnerability research, penetration testing, reverse engineering, malware analysis and forensics tasking. He then went on to lead a highly skilled team focused on a wide spectrum of internal and external security assessments for Fortune 500 companies at a consulting firm Protiviti.

Douglas is a skilled speaker and teacher and throughout his career has provided software exploitation training to many audiences, including law enforcement. Douglas is a regular at major industry conferences such as DEFCON and currently holds many well-known industry certificates including the GREM, OSCP and GXPN; his research is frequently featured in industry publications. Douglas McKee obtained his Master of Science in Information Security from East Stroudsburg University.

Douglas McKee

@fulmetalpackets

# Mark Lechtik

Mark Lechtik is a Senior Security Researcher at Kaspersky`s GReAT, previously working as the Malware Research Team Leader at CheckPoint Research. He was born in Russia, but has lived most of his life in Israel, where he graduated from Ben-Gurion University with a B.Sc in communication systems engineering. Mark's passion is reverse engineering of malware, and sometimes goodware - especially when it comes to North Korean software. He spends most of him time deep diving into a variety of malwares from the worlds of both APT and crimeware, digging out their gory technical details and outlining their underlying stories and threat actors.

Mark Lechtik

@_marklech_

# Fumik0_

Fumik0_ is a self-taught independent malware researcher who has been noticed multiple times, by unveiling malware that are nowadays pretty active in the wild like Vidar, Predator the thief or Qulab. He is mostly interested about how threat actors are developing their products by performing in-depth analysis on them and publishing the results on his blog. He is also behind a malware tracker designed to provide samples, memos and exercises for free with the main focus to provide for the community, the opportunity to learn and assimilate easily some malware fundamentals, without being overwhelmed with unnecessary data or being forced to pay for some access.

Besides this, he is easily recognized by his true love for the Japanese culture and the demoscene, and considering malware analysis more like a hobby than an actual serious thing.

@fumik0_

fumik0.com

/tracker.fumik0.com

# Silas Cutler

Silas Cutler joined Google/Chronicle Security in October 2018 as Reverse Engineering Lead to support technical analysis from targeted attacks.  Building on prior work from CrowdStrike and Dell SecureWorks, Silas specializes in reverse engineering malware artifacts, threat hunting, and development of tools to track actor operations.

@silascutler

# MalwareTech (Marcus Hutchins)

Marcus Hutchins, also known online as MalwareTech, is a British computer security researcher known for temporarily stopping the WannaCry ransomware attack. He is employed by cybersecurity firm Kryptos Logic. Hutchins is from Ilfracombe, Devon, UK. He runs a very popular blog "MalwareTech - Life of a Malware Analyst".

MalwareTech

MalwareTech

# William Meyers

William has a decade and a half of experience within the field of information security. He has supported a fortune 5 company as a security engineer, supported many government and commercial customers in various roles within a Security Operations Center (including Incident Response analyst, DMA Lead and SOC Manager) and now is a Principal Security Researcher in a malware analysis role. He has taken the initiative to mentor and train new team members and has led many community events within the companies he has worked for. These events include quarterly mini conferences, Capture The Flag (CTF), and other events to build the community and share knowledge. William is currently a SANS mentor and currently holds the OSCP, CISSP, GCIA, GCIH, GPEN, GREM, GCTI, and GXPN GIAC certifications.


William Meyers

@_hAxel

# Michael Gillespie

My name is Michael Gillespie, aka Demonslay335, and I am an independent security researcher / programmer. In my free time, I primarily focus on analyzing (and trying to break) ransomware, and helping victims recover their data when possible. I built and run the website ID Ransomware, which helps victims worldwide identify what ransomware encrypted their files, and if there is a known way of decrypting them. In 2017, I received the Director's Community Leadership Award from the FBI, and in the past few years, have written free decryptors for nearly a hundred ransomware.

@demonslay335

# Brian Baskin

Brian Baskin is a Threat Researcher with a specialty in digital forensics, incident response and malware analysis. For 20 years he has helped discover, develop, and demonstrate new techniques for security analysts and incident responses. Many of his years were at the US Defense Cyber Crime Center where he trained military and federal law enforcement agencies in digital forensics, while providing services to help augment their analysis. He also worked as an Intrusions Analyst for the Center where he focused on large-scale network intrusions and reverse engineering new malware and attacks. Brian uses his years of incident response and research work to study new attacks as they come out and to help mentor new analysts joining the industry.

Brian has spoken at conferences around the world including RSA, RSA APJ, FIRST, GFIRST, and DerbyCon. He helped lead Security BSidesCharm, an extremely popular security conference in Baltimore, Maryland. He led a "Law Enforcement" team at the MidAtlantic Collegiate Cyber Defense Competition (MACCDC), teaching students the value of performing malware triage and forensics while under stress. Brian has also guest lectured at universities and was a Subject Matter Expert in the design of courses at the Federal Law Enforcement Training Center (FLETC) and the National White Collar Crime Center (NW3C). He has authored multiple computer security books and maintains multiple open source tools for malware analysis and digital forensics.

Brian Baskin

@bbaskin

ghettoforensics.com

github.com/Rurik

# Seongsu Park

Seongsu Park is a passionate researcher on malware research, threat intelligence, digital forensics and incident response with over 10 years of experience in cybersecurity. He has extensive experience in malware research, evolving attack vectors researching, and threat intelligence with a heavy focus on response to nation-state adversary attacks. He's mostly tracking high-skilled Korean-speaking threat actors.

Now he is working in the Kaspersky Global Research and Analysis Team(GreAT) as a senior security researcher and focuses on analyzing and tracking security threats in the APAC region.

Seongsu Park

@unpacker

# Luca Mella

Luca is a Cyber Security professional with deep passion for hacking and intimate curiosity for the digital world. He is a former member of the "ANeSeC" CTF team, one of the first Italian war-game teams born back in 2011. His curiosity and passion turned into a career when he joined the Italian cyber security startup "Yoroi". Currently, Luca is a member of the CERT-Yoroi and collaborates within the Italian and the European CSIRT community.

Luca's experience ranges from highly technical activities like Malware Analysis and Incident Response to Threat Intelligence and Information Security Management Systems standards.

Luca also believes in the value of the continuous learning and in the centrality of knowledge and information sharing as the key strategy to improve the resilience of the cyberspace. He is also active is the divulgation of security and privacy culture participating and supporting nonprofit associations and collaborating with Italian online news media such as CyberSecurity360.

Luca Mella

@luc4m

https://lucamella.space/

# Clay Dunnavant

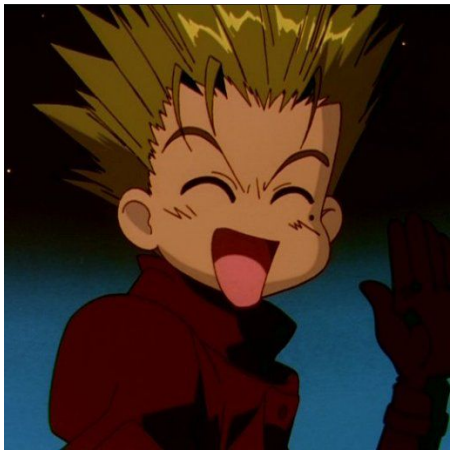
My name is Clay and I've been an Information Security Analyst for an entertainment and hospitality company in the Milwaukee area for just over two years. My interests primarily include log analysis, email security, and DFIR. Since I entered the InfoSec Field, I have been constantly drinking from the fire hose so to speak. I love the industry I'm in because of all the rabbit holes I'm able to go down.

Clay Dunnavant

@SecSome

Early in my career I have noticed that many of the phishing events I was seeing were not being reported on. That's when I realized that this issue is much bigger than just the small number of (remarkable) individuals reporting on them. Sharing is caring. That's why I created my Twitter handle. Personally I'm not a huge fan of social media but I can now see how sharing what I'm seeing on a daily basis can be helpful for many users across the InfoSec industry.

# Pollo290987



Pollo290987 have been working for many years in pretty much all facets of security, mostly from a purple perspective. Part of their experience include reverse engineering, Linux administration, Active Directory, botnets, and incident response.

Pollo290987 is well known in the malware analysis and reversing community. Particularly interested in Emotet, but by no means only in that. He has set up SOCs and had a very active role in significant Incident Response events. Well versed in botnets, malware , threat intelligence and osint. Always studying the latest techniques and tools for evasion and detection. Very protective of his privacy and RL details.

@pollo290987

# Albert Zsigovits

Albert works as a Threat Researcher at Sophos.

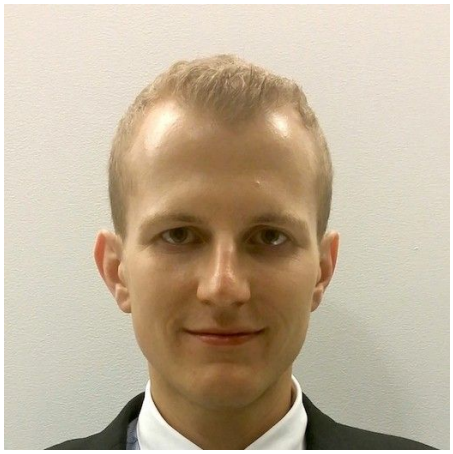
He joins Sophos from a traditional blue team background, kickstarting his cyber career analyzing security events as an IDS analyst, and later investigating breaches as an incident responder for a Fortune 50 company.

His specialities include threat hunting, memory forensics and signature development. In his spare-time he enjoys reverse engineering malware and diving deep into deep-web territories, connecting the dots between criminals leveraging threat intelligence and open source intelligence techniques.

Albert Zsigovits

@albertzsigovits

# Vitali Kremez



Vitali leads a subject matter expert technical team that specializes in researching and investigating complex cyber attacks, network intrusions, data breaches, and hacking incidents. Vitali is a strong believer in responsible disclosure and has helped enterprises and government agencies deliver indictments of many high-profile investigations involving data breaches, network intrusions, ransomware, computer hacking, intellectual property theft, credit card fraud, money laundering, and identity theft. Previously, Vitali enjoyed a rewarding career as a Cybercrime Investigative Analyst for the New York County District Attorney's Office.

He has earned the majority of certifications available in the information technology, information security, digital forensics, and fraud intelligence fields. A renowned expert, malware course author, speaker, blogger, and columnist, Vitali has contributed articles to Dark Reading, BusinessReview, and Infosecurity Magazine and is a frequent commentator on cybercrime, hacking incidents, policy, and security.

To beat a cybercriminal, you have to think like one.

Vitali Kremez

@VK_Intel

http://vkremez.com

# Jaromir Horejsi

Jaromir Horejsi is a threat researcher at Trend Micro. He specializes in hunting and reverse-engineering threats that target Windows and Linux. He has researched many types of threats over the course of his career, covering threats such as APTs, DDoS botnets, banking Trojans, click fraud and ransomware. He has successfully presented his research at RSAC, Virus Bulletin, SAS, FIRST, AVAR, Botconf and CARO.

@JaromirHorejsi

# Ruben shotgunner101

My name is Ruben and my twitter handle is @shotgunner101 . I have worked professionally within in Cyber Security now for 4 years. I work at a fortune 50 and love everyday as I always get to learn new things, find new threats, etc. I also run my own personal website located at https://dodgethissecurity.com . I love finding weaknesses in threat actors campaigns and being able to throw kinks in their normal operations.

One of my favorite things to do is to research malware, its behavior, how it changes over time, and find ways to both detect it as well as help predict its future changes. Overall I would say working in InfoSec has been a challenging yet very rewarding experience thus far. I am looking forward to where this career will lead me down the road.

@shotgunner101

Dodge This Security

# That_malware_guy

Independent Security researcher with experience and expertise in Intelligence and other aspects of security fields such as Malware analysis, Attribution and financial crimes.

@makflwana