SANS

Open-Source Intelligence

Summit 2019

Program Guide

@SANSDefense #OSINTSummit

Agenda

All Summit Sessions will be held in the Ballroom A/B (unless noted otherwise).

All approved presentations will be available online following the Summit at ***sans.org/summit-archives***

Monday, February 25

7:00-9:00 am	**Registration & Coffee** (LOCATION: BALLROOM FOYER)
9:00-9:15 am	***Welcome & Opening Remarks*** ***Micah Hoffman*** *(@WebBreacher), Summit Chair, SANS Institute*
9:15-10:00 am	***Keynote: So, You Want to OSINT Full-Time*** What does it take to turn OSINT into a career? Kirby Plessas, an Army veteran, trained linguist, and DHS-designated "technical expert," regularly consults with intelligence agencies, law enforcement entities, and corporations, teaching them how to leverage open source research. She'll share her experience and wisdom on building your brand and even your own business as an OSINT specialist. If open source intelligence is your passion, Kirby will introduce you to the world of opportunities. ***Kirby Plessas*** *(@kirbstr), Founder & CEO, Plessas Experts Network, Inc.*
10:00-10:25 am	**Networking Break** (LOCATION: BALLROOM FOYER)
10:25-10:55 am	***OSINT: Breach Data, Ethics, and OpSec... Oh My!*** This talk will examine the use of breach data in OSINT investigations. What do breach data look like? Are breach data ethical? How can they be used? What do breach data teach us about privacy and security awareness? What can we do to protect our own data against a breach? Using real-world examples, we'll discuss these questions and provide resources you can use to leverage breach data in your own investigation. ***Josh Huff*** *(@baywolf88), OSINT Investigator*
10:55-11:00 am	***Q&A***
11:00-11:30 am	***Backdoors to the Kingdom: Changing the Way You Think about Organizational Reconnaissance*** Most current reconnaissance methodologies – such as Domain Name System enumeration, subnet scanning, reliance on Whois Data, and knowledge of owned Autonomous System Numbers (ASNs) or netblocks – are still targeting wells that are drying up or are no longer relevant. The European Union's General Data Protection Regulation has removed access to most Whois data, and moving to the cloud has reduced organizational presence on owned ASNs. But you can still map out an organization if you know where to look. No matter the objective of your team (red, blue, or purple) it's important to know where the security and/or visibility gaps are. We are only here to find things – we'll leave the resolutions/mitigations/code development and go-dead workflows to your architecture and application teams. This talk will highlight truly passive reconnaissance utilizing often-overlooked open-source data – all without ever touching a domain. ***David Westcott****, Security Principal – Threat Hunting, OSINT & Reconnaissance (THOR), iDefense*
11:30-11:35 am	***Q&A***

Monday, February 25

11:35 am – 12:05 pm	***From the Mean Streets to the Information Superhighway: Lessons Learned as a Private Investigator*** This talk will offer Insights into investigations from the perspective of a cyber analyst with a background as a private investigator. The presentation will draw on years of experience in the field and in front of a keyboard to make connections between the worlds of physical security, "old-school" OSINT, and field investigations of cyber and Internet OSINT. We'll also provide some thoughts on useful investigative processes, techniques, and "gotchas" that may shift your perspective on how to manage and conduct OSINT investigations. ***John TerBush*** *(@thegumshoo), Senior Threat Intelligence Researcher, Recorded Future*
12:05-12:10 pm	***Q&A***
12:10-1:30 pm	**Lunch** (LOCATION: BALLROOM C)
1:30-2:00 pm	***Weaponizing OSINT*** We need to explore the malicious side of OSINT. As professionals, we should discuss the action of using data against people, see the attacker side, and review the ease of locating information valuable enough to be used against someone. This includes a truly passive attack with no code being launched at the targets, and even getting at the target through passive means. The material involved doesn't have to include data dumps of paid dating or porn sites. Health records, online groups/forums, and even social media might have an effect on a target's future. Now that more data points are surfacing on many different levels, it is more possible to pattern targets. What if a person was profiled? What about a large corporate target's brand? What about people asking for job material or looking for a new career? What would people pay to not have stuff known? In this presentation, we'll investigate embarrassing ways to make sure that the target notices, and we'll also travel down other attack paths. The point of the talk is: attack to defend. Every case may be different, but we'll look at some basic steps that targets can take to help their online presence. Only by knowing that there is a problem can we defend against it. ***Michael James*** *(@ginsberg5150)*
2:00-2:05 pm	***Q&A***
2:05-2:35 pm	***Hunting Down Malicious Sites Using Certstream Data and Available Web Services*** A number of automated tools now provide for analytics of new SSL certificate registration to watch for sites that may be spoofing the brands of a company or organization in order to create phishing domains that bypass DMARC, camouflage command and control infrastructure, or undertake other nefarious purposes. In this presentation we will walk through one of these tools – StreamingPhish by Wes Connell – and look at a number of other web-based services that can be used to hunt down possible malicious look-alike sites. ***Sean Gallagher*** *(@thepacketrat), IT Editor/National Security Editor, ArsTechnica*
2:35-2:40 pm	***Q&A***
2:40-3:00 pm	**Networking Break** (LOCATION: BALLROOM FOYER)

Monday, February 25

3:00-3:30 pm	***Beginner's Business and Legal Research*** If you were asked to look at a company's 8-K or to find a Writ of Certiorari, would you know what to do? Harness the power of OSINT in this session to learn the basics of finding business and legal information. Get an understanding of the resources available, key terms, and in some cases, what you can actually do with the information you find. Gain insight into research from a former law firm librarian to feel more at ease with these often confusing industries. Users will leave this session with a foundation of where to find business and legal information, terminology, and applications of the knowledge gained. ***Tracy Z. Maleeff*** *(@InfoSecSherpa), Cyber Analyst*
3:30-3:35 pm	***Q&A***
3:35-4:15 pm	***Using OSINT to Improve Critical Business Decision-Making*** Thorough due diligence is a game changer for any organization considering an acquisition, merger, or c-suite hire. It can also be the critical difference between getting a hefty return on an investment versus writing off a loss. In this presentation, we will discuss how organizations should leverage open-source intelligence (OSINT) to identify risks, threats, and opportunities – thereby facilitating well-informed decisions that affect the future of an organization. ***Tazz*** *(@GRC_Ninja), Threat Intelligence Advisor, Divine Intel, LLC*
4:15-4:20 pm	***Q&A***
4:20-4:55 pm	***The OSINTCurio.us Project*** In January 2019, several members of the OSINT community created an online learning site focused on solid, actionable OSINT tips, tricks, events, and techniques. This is a diverse group of experts from Cyber Threat Intelligence (CTI) to Private Investigation (PI), cyber penetration testing to cyber defenders who make available regular webcasts/podcasts focused on OSINT, a Google calendar with OSINT events and trainings, and blog about a variety of topics that matter to OSINT investigators and enthusiasts alike. This informal Q&A panel will pique your curiosity! Come with questions or ask on Twitter with the #osintcurious hashtag. MODERATOR: ***Micah Hoffman*** *(@WebBreacher), Summit Chair, SANS Institute* PANELISTS: ***Ginsberg5150*** ***Josh Huff*** *(@baywolf88), OSINT Investigator* ***Kirby Plessas*** *(@kirbstr), Founder & CEO, Plessas Experts Network, Inc.* ***John TerBush*** *(@thegumshoo), Senior Threat Intelligence Researcher, Recorded Future*
4:55-5:00 pm	***Closing Remarks***
5:00-6:30 pm	***Post-Summit Networking Reception*** (LOCATION: GRAND BALLROOM FOYER) Join us for food, drinks, and networking in the Ballroom Foyer.

Thank you for attending the SANS Summit.

Please remember to complete your evaluations for today.
You may leave completed surveys at your seat or turn them in to the SANS registration desk.

@SANSDefense  **#OSINTSummit**