DeepSec GmbH
✉Bräuhausgasse 32
✉1050 Wien - Austria
✉deepsec@deepsec.net
✆+43.676.5626390 ✆+43.720.349387 🖷+43.720.34938723

DeepINTEL Speakers and Supporters
Planet Earth

DeepINTEL 2020 - Call for Papers

16 February 2020

Dear ladies and gentlemen,
the next DeepINTEL Security Intelligence Conference will be this year on **18 November 2020** in **Vienna, Austria**. The day is the second day of trainings of the DeepSec 2020 In-Depth Security Conference.

We are calling for presentations on security intelligence. The focus for 2020 are case studies of successful attacks, capabilities of adversaries, and metrics of threat analysis. The IT environment has evolved. The Internet of Things is spreading. Access technology has pushed more devices, organisations, and individuals online. Most software now lives in a world filled with ubiquitous networking, complex trust-relationships, and the increased flow of information between all kinds of platforms, services, layers, and parties.
We are still interested in analysing aspects of combined operations where social engineering, disinformation, attacks on digital infrastructure, and abuse of data are chained together. Ubiquitous networking, complex trust-relationships, use of social media, and the steady flow of information from the inside to the outside is the perfect stage for these advanced threats. During the past years a number of attacks have been tied to a geopolitical context. Operations of nation states are part of the threat landscpae even for smaller organisations and enterprises. Furthermore, cybercrime plays a role next to nation state agendas. The incidents landing on the doorstep of security operations centres may be a result of both worlds. It is increasingly difficult to clearly distinguish between both areas given the technological capabilities of the adversaries. Attribution is hard, but it is impossible without an in-depth analysis of all available (and retrievable) information.

We would like to discuss past and present threats in this context based on data from actual events.

We regard security intelligence as any information exceeding classic techniques which enables any IT security team to choose better strategies and thus to defend information infrastructure more efficiently. At DeepINTEL we discuss security intelligence and related topics within a closed group. DeepINTEL is not an event open to the public, but a seminar where strategies to deal with contemporary problems of information security are being discussed.
The conference will be open to a limited audience only. All participants, including speakers and delegates, are vetted. One of our trust anchors is the www.trusted-introducer.org community, all listed members and organizations are whitelisted. We ourselves have applied for the TI

DeepSec GmbH
✉Bräuhausgasse 32
✉1050 Wien - Austria
✉deepsec@deepsec.net
✆+43.676.5626390 ✆+43.720.349387 🖷+43.720.34938723

Affiliate status. We will accept individuals vetted for by TI community members. Furthermore we will screen all participants with the help of our partners CERT.at. DeepINTEL Speakers will receive the list of participants prior to the conference.
We expect talks with the Traffic Light Protocol level Amber[1] clearance (**TLP:AMBER - Limited Distribution**). This is why we have choosen a closed format for DeepINTEL. Of course you can also present public content in your presentation provided it suits the context. All speakers and participants have to agree on sharing information accordingly.
A few examples for topics (not limited to) are:

- Attribution of adversaries
- Building honeypots to gain security intelligence, e.g. through „tainted data“ and tracking access
- Capabilities of adversaries
- Case studies of (documented) incidents
- Case studies of successful attacks or attack attempts
- Connections between adversary groups (such as cooperations; for assessing capabilities or intentions)
- Detection of threats not efficiently covered by classic solutions
- Forensic techniques or results, revealing additional background of an incident
- Insight into the black market
- Malware analysis for better assessment of the intention of adversaries
- Projects, systems, or methods to automatically exchange and/or distribute security intelligence information to a limited audience
- Psychology of adversaries (e.g. social engineering, profiling, assessment)
- Use of (targeted) disinformation

What we are **not** looking for (there are other, more suitable events covering this):

- Surveillance technology (new or otherwise)

[1] https://www.us-cert.gov/tlp

DeepSec GmbH
✉Bräuhausgasse 32
✉1050 Wien - Austria
✉deepsec@deepsec.net
✆+43.676.5626390 ✆+43.720.349387 🖷+43.720.34938723

DEEPSEC

- Love stories about your favourite tool (regardless if this is an algorithm, software, hardware, . . .)
- Any classic approach like off-the-shelf SIEM, vulnerability scanning or firewall solutions, regardless how „next-generation“ they are; if they don't employ significantly security intelligence like mentioned above
- Statistics – mindlessly counting damages, scores, incidents, etc.; mathematics and algorithms are fine, but not limited to the field of statistics. Proper threat and security intelligence needs meaningful metrics. If you have that, no problem. If not, problem.
- „Cyber“, „cyber“, „cyber“, . . .
  The term *cyber* is constantly misused in the media, politics, even computer science; and it is often used to cloak lack of understanding, an agenda, or simply lacking a well-defined meaning. If you are going to use this word, please make sure you state clearly what you are talking about. This holds true for any other prominent term used in social networks or the media.

All DeepINTEL speakers also get free access to the DeepSec conference. It's easier to process new information when you have the time to talk to peers.

We strongly encourage you to submit papers (PGP-/GPG-)encrypted to our general key

```
deepsec@deepsec.net

PGP/GPG key id: 0x49CE0CBEC210A5CE
Fingerprint   : E45E B86D A50C 3F6C 295A  1CCF 49CE 0CBE C210 A5CE
```

or to my key directly:

```
rpfeiffer@deepsec.net

PGP/GPG key id: 0x518A0576C3A9FF76
Fingerprint   : AEC5 5A46 90F8 F6FD CF55  C965 518A 0576 C3A9 FF76
```

We also use Signal and Threema for communication. You can find the full contact information on our web site. In addition we offer secure communication via the GSMK Cryptophone™ technology:

- DeepSec office – +807.911.52.401
- René Pfeiffer, mobile phone – +807.949.050.59

DeepSec GmbH
✉Bräuhausgasse 32
✉1050 Wien - Austria
✉deepsec@deepsec.net
+43.676.5626390 +43.720.349387 +43.720.34938723

Please get into contact to verify identification of accounts or telephone numbers. Of course plaintext submission will be accepted, too. However we advise not to use insecure channels for sensitive information.
And please refrain from sending us any (sensitive) information by means of social media or business networks regarding the DeepINTEL event. The contact information we provide here is just fine.

Hope to hear from you soon!

Best regards,
René „Lynx“ Pfeiffer,
Managing Director (+43.676.5626390, GSMK Cryptophone™ +807.949.050.59),
DeepSec Conference Organisation Team.