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

DEEPSEC

DeepINTEL Speakers and Supporters
**Planet Earth**

## DeepINTEL 2018 - Call for Papers

10. August 2018

Dear ladies and gentlemen,
the next DeepINTEL Security Intelligence Conference will be this year on 28 November in Vienna, Austria. The day is the second day of trainings of the DeepSec 2018 In-Depth Security Conference.

We are calling for presentations on security intelligence. The focus for 2018 are stealthy and persistent attacks. This is the classic espionage attack vector, only with modern means. Ubiquitous networking, complex trust-relationships, and the increased flow of information (and code) is the perfect breeding ground for advanced and persistent threats. We would like to discuss past and present threats in this context without the hype. Essentially we like to focus on (industrial) espionage and methods of nation state actors.

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. Our trust anchor is basically www.trusted-introducer.org, all listed members and organizations are whitelisted. We will accept individuals vetted for. Speakers will receive the list of participants prior to the conference.
We expect talks with the Traffic Light Protocol level Amber[1] clearance. 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.
A few examples for topics (not limited to) are:

- Attribution of adversaries
- Malware analysis for better assessment of the intention of adversaries
- Capabilities of adversaries
- Connections between adversary groups (e.g. for assessing capabilities or intentions)

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

- Detection of threats not efficiently covered by classic solutions
- Projects, systems, or methods to automatically exchange and/or distribute security intelligence information to a limited audience
- Forensic techniques or results, revealing additional background of an incident
- Building honeypots to gain security intelligence, e.g. through „tainted data“ and tracking access
- Insight into the black market
- Case studies of (documented) incidents
- Psychology of adversaries (e.g. social engineering, profiling, assessment)

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

- Surveillance technology (new or otherwise)
- 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, incidents, etc.; mathematics and lagorithms are fine, but not limited to the field of statistics
- 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 we 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 prominent term used in social networks or the media.

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
```

We also use Signal and Threema for communication. You can find the full contact information on our web site. Please get into contact to verify identification of accounts or telephone numbers. Of course plaintext submission will be accepted, too.
And please refrain from contacting us with sensitive information by means of social media or business networks. 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),
DeepSec Conference Organisation Team.