Deloitte.

# Cyber Flash

## A spotlight on cyber and privacy trends

Edition 1, December 2016

# Editorial

## Edition 1, December 2016

Dear Cyber and Privacy Community

Welcome to the first edition of our Cyber Flash – a quarterly spotlight on Swiss and global cyber security trends and regulatory developments.

As we reach the end of 2016, I would like to highlight a few key issues and developments the Swiss and global marketplace faced this year that will continue to have an impact on your daily business in 2017 and beyond.

The fast growing trend towards a digital economy offers an ideal breeding ground for sophisticated cyber threat actors. Personal data, intellectual property, critical infrastructure and - as we have seen in the case of the cyber espionage on the Iran nuclear deal negotiations in Geneva - even military and national security can be compromised. This makes it crucial to stay on top of the latest Advanced Persistent Threat developments and to have a plan in place to protect your organisation.

Furthermore, the formal publication of the new GDPR text earlier this year, brought on a flurry of privacy and data protection related activities across Europe, which you need to be aware of this winter. This news flash provides a brief summary.

On behalf of our Cyber Risk Services team I would like to thank you for your trust and ongoing relationship, and wish you an interesting read.

Season's Greetings and our sincere best wishes for 2017.

Yours sincerely,

## Highlights, issue 1

### Cyber security

- Advanced Persistent Threat (APT) – latest developments, potential impacts and recommendations
- Cyber espionage at nuclear deal negotiations in Geneva

### Privacy and data protection

- Towards data-centric security: Enterprise Digital Rights Management (EDRM)
- Privacy issues you need to be aware of this winter
- Events, conferences and contacts

**Mark Carter**
**Managing Partner**
**Risk Advisory**

# Cyber security

## Advanced Persistent Threat

### Latest developments, potential impact and recommendations

"Advanced Persistent Threat" (APT) is probably one of the most hyped phrases since Mandiant published one of the first reports about such a sophisticated threat actor group in 2013[1]. Now in 2016 we see "APT reports" almost monthly and all the interesting facts and details get lost in a lot of media and marketing hyperbole. This article provides a crisp explanation of APTs and summarises the latest developments with recommendations to protect your organisation.

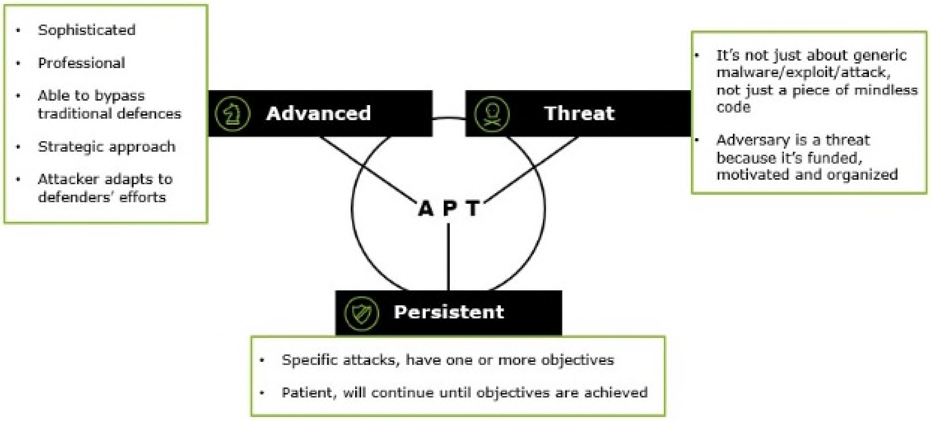
Sophisticated
Professional
Able to bypass traditional defences
Strategic approach
Attacker adapts to defenders' efforts
Advanced
Threat
It's not just about generic malware/exploit/attack, not just a piece of mindless code
Adversary is a threat because it's funded, motivated and organized
A P T
Persistent
Specific attacks, have one or more objectives
Patient, will continue until objectives are achieved

Figure 1: Advanced Persistent Threat explained.

### What does it mean?

APT stands for **A**dvanced **P**ersistent **T**hreat, describing a non-opportunistic group breaching organisations in a strategic, long-term manner with clear objectives. In addition, they will not easily be deterred in their actions until they have achieved what they set out to do. The following graphic-provides a brief explanation of each term.

In simple words, APTs are the **"cyber hulks"** out there and totally differ from the opportunistic threat actors who, for example, are only looking to steal some credit card data for short term gain. Moreover, an APT is never just a random piece of malware even though they do sometimes use sophisticated self-made software for their attacks. APTs are dangerous because of the people behind the operation - those who plan and run the APT campaigns and control the tools.[2]

### Latest developments

The "APT1" report Mandiant published in 2013 resembled the opening of a hunting season on APT groups. Organisations around the globe - such as Kaspersky, CrowdStrike, HP, TrendMicro, to name only a few - started publishing details about identified APT groups like "Putter Panda", "FancyBear", "KungFu Kittens" and "Playful Dragon". And the hunting season is far from over.

Since then, these organisations have identified more than 150 APT groups globally. Thanks to these reports, the industry is not only aware of the evolving threats, but now also has details on their tactics, techniques and procedures. Unfortunately it seems that there has not been much change in tactics in recent years. This might be because APT groups are still successful with their current approach consisting of:

- **Targeted phishing attacks** via e-mails and watering hole attacks
- **Custom-made malware** with different infection stages
- **Exfiltration** via DNS, HTTP POST and similar

The only things that have been evolving in recent years are:

- APT groups **no longer go dark** after successful campaigns
- **Decreasing persistence**
- **Increasing usage of native OS** tools for operations

[1] Mandiant: APT1 – Exposing One of China's Cyber Espionage Units (2013)

[2] http://www.scmagazineuk.com/black-hat-attendees-na%C3%AFve-on-advanced-persistent-threats/article/450210/ (accessed 19.09.2016)

Our first observation of **"going dark"** refers to a group shutting down its infrastructure and immediately discontinuing all activities as soon as they achieved their objectives and/or security researchers detected them. Seeing this behaviour change is surprising. One would assume that an APT group would go dark, vanish and stay hidden to protect itself from detection. The first big campaigns showed exactly this operating pattern; recently, however, groups continue their activities after their public disclosure. In fact, it seems like they immediately use the gained information against new targets and move on seamlessly. This operating model offers an excellent opportunity to prepare and defend. Because now APT actors/groups can be better identified by their infrastructure, tactics, techniques and procedures – as long as they are detected quickly and organisations exchange threat intelligence quickly.

The second development can be distinguished from entries in the "Targeted Cyberattacks Logbook"[3]. While the number of campaigns is rising, their length is actually decreasing. The Carbanak group - also known as Anunak group - illustrates this tendency. This group is spending only 42 days on average within a target network until it fulfilled its objectives.[4] For such short timeframes, a fast detection and rapid response is crucial.

The third and last observation is the increasing usage of native operating system tools like **powershell, commandline, psexec** and others. One explanation for this phenomenon may be the very stealthy nature of these tools, as most companies do not monitor their usage and AV systems do not report them as malicious. In addition, they are very powerful and cheaper to use – compared to custom-made, self-engineered malware, as security researchers will detect and flag ("burn") them quickly during the ongoing "APT hunt". A prominent example where threat actors compromised an organisation and stole dozens of gigabytes of data with the help of OS tools recently made headline news in Switzerland[5]. Given this pressure resulting out of this "APT hunt", we might see memory-only malware in the future for APT campaigns, which has been predicted by industry insiders for some time. In fact, for malware such as the Mirai DDoS Bot, memory-only versions already exist, where a reboot clears the device. As a more sophisticated version of Mirai (called "Hajime") is in the wild, we might witness APT campaigns that have custom memory-only malware in their repertoire as well.

Detection is key for APTs, and there are a couple of simple concepts that many companies do not yet implement systematically, but that are crucial to detect a compromise:

- **Logging.** Log proxy events, webserver events, DNS, AV events (yes, also "cleaned" and "moved to quarantine" events), store all in a central location and have your security teams review them.
- **Monitor** the usage of native OS tools like **powershell** and **psexec**. The average user does not need them.
- **Use Two-Factor Authentication** wherever possible, including high-privileged Active Directory accounts.

Even though these groups are labelled as "advanced", it does not mean you have no chance to protect your data against them. In many cases, you cannot protect yourself from an infection, but the infection itself and the compromise in your network always leave traces that can be detected and acted upon.

**Felix Rieder**
**Senior Consultant**
**Risk Advisory**
+41 58 279 6515
Email

[3] Targeted Cyber Attack Logbook https://apt.securelist.com/#secondPage (accessed 17.11.2016)
[4] Anunak APT https://www.fox-it.com/en/files/2014/12/Anunak_APT-against-financial-institutions2.pdf (accessed 17.11.2016)
[5] RUAG APT Case, technical report https://www.melani.admin.ch/melani/en/home/dokumentation/reports/technical-reports/technical-report_apt_case_ruag.html (accessed 16.11.2016)

## Cyber espionage at nuclear deal negotiations in Geneva

# Government organisations targeted by advanced cyber threat actors

The world has changed. A few hundred years ago spies relied on infiltrating organisations in person and a dozen years back they could at least install bugs.

Nowadays nearly every electronic device can be turned into a bug to eavesdrop on anything that happens around them – in addition to the ability to steal digital communication and files.

This reality finally sunk in when the office of the attorney general in Switzerland ("Schweizer Bundesanwaltschaft") recently confirmed an attack on the nuclear deal negotiations with Iran. Parts of the negotiation took place in a conference hotel in Geneva, which was compromised by an unknown threat actor using a sophisticated malware called "Duqu 2.0"[6].
Based on today's knowledge this malware belongs to a so-called „Advanced Persistent Threat" (APT) campaign. The same group responsible for developing the "Stuxnet" Trojan is suspected to also have developed this "Duqu 2.0" dubbed Trojan. Most of the activities by this group seem to target Iran. Stuxnet sabotaged Iran's nuclear programme by infecting the processor controlling the centrifuges that separate nuclear material. The Duqu 2.0 Trojan is mostly used for intelligence gathering attacks. It can be assumed that this Trojan was built with the specific purpose of information exfiltration / intelligence gathering based on its functionality and the discovered modules.[7]
Currently more than 150 active APT campaigns have been identified around the globe; some of them solely targeting government organisations:[8]

- **APT6** targets government organisations of the United States of America9
- **Hellsing** is an APT campaign with focus on Vietnam and other governments in South Asia[10]
- **SVCMONDR** is targeting governments in Kazakhstan, Kirgizstan, Uzbekistan, Myanmar, Nepal, Philippines and India.[11]
- **Hammer Panda** has a clear focus on Russian organisations.[12]

A look at all these campaigns confirms that government organisations are under attack – and it is not a recent development, but instead has been going on for quite some time already. If the "APT" topic may have seemed a distant concern in the past, the above as well as the recently confirmed attack on Ruag in Switzerland have caused a shift in perception: the threat is real, close by, and affects everyone including governments and nation states. Are you prepared and taking all the necessary precautions to be secure?

For further information about APTs, please revert to our "APT's latest developments" article in this Cyber Flash.

**Felix Rieder**
**Senior Consultant**
**Risk Advisory**
+41 58 279 6515
Email

[6] Schweizer Bundesanwaltschaft bestätigt Spionagetrojaner bei Atomverhandlungen, http://www.heise.de/newsticker/meldung/Schweizer-Bundesanwaltschaft-bestaetigt-Spionage-Trojaner-bei-Atomgespraechen-3456012.html (accessed 16.11.2016); Cyber-Spionage bei Atomkonferenz in Genf, http://www.srf.ch/news/international/cyber-spionage-bei-atomkonferenz-in-genf (accessed 16.11.2016)

[7] The Mystery of Duqu 2.0, https://securelist.com/files/2015/06/The_Mystery_of_Duqu_2_0_a_sophisticated_cyberespionage_actor_returns.pdf (accessed 19.11.2016)

[8] APT Groups and Operations, https://docs.google.com/spreadsheets/d/1H9_xaxQHpWaa4O_Son4Gx0YOIzlcBWMsdvePFX68EKU (accessed 19.11.2016)

[9] APT6, https://motherboard.vice.com/read/fbi-flash-alert-hacking-group-has-had-access-to-us-govt-files-for-years (accessed 22.11.2016); https://www.zscaler.com/pdf/technicalbriefs/tb_advanced_persistent_threats.pdf (accessed 22.11.2016)

[10] The Chronicles of the Hellsing APT, https://securelist.com/analysis/publications/69567/the-chronicles-of-the-hellsing-apt-the-empire-strikes-back/ (accessed 22.11.2016)

[11] Recent APT threats, https://securelist.com/analysis/publications/74828/cve-2015-2545-overview-of-current-threats/ (accessed 22.11.2016)

[12] Chinese Cyberspies Pivot To Russia In Wake Of Obama-Xi Pact, http://www.darkreading.com/endpoint/chinese-cyberspies-pivot-to-russia-in-wake-of-obama-xi-pact/d/d-id/1324242 (accessed 22.11.2016)

# Privacy and data protection

## Towards data-centric security: Enterprise Digital Rights Management (EDRM)

Digital transformation efforts typically aim at achieving improved customer experiences, seamless collaboration between employees and partners, and automation through M2M (Machine-to-Machine) communication, e.g. IoT. As such, they foster digital ecosystems that include mobile and cloud solutions, as well as data transfers across multiple networks, platforms, people, applications and services.

As corporate boundaries erode, a traditional perimeter-based security may not be able to effectively protect companies' data assets. To address this growing risk, there is a need to apply protection on the data level and to secure data throughout the entire lifecycle, i.e. when it is created, stored, used or exchanged between employees, partners and external parties, until it is finally archived or deleted.

As Deloitte cyber security practitioners, we witness a growing interest in data-centric security among our clients. A technology that has gained particular popularity and that frequently appears on our customers' security roadmaps is **Enterprise Digital Rights Management (EDRM)**. EDRM technology has been around for several years, but its availability on mobile devices and compatibility with widely used collaboration and email platforms enabled its recent expansion. It is a combination of identity and access management and encryption. EDRM-protected content is encrypted and coupled with a protection policy that specifies permissions for different users and user groups, such as view, edit, download, print, save or forward. For a user to access protected content, authentication is needed. Based on the identity, the user is granted permissions in accordance with the protection policy. In contrast to a traditional, application-oriented identity and access management solution, EDRM protection stays with the content and ensures it is secured independently of the application, device or access location. EDRM is typically used to protect highly sensitive documents and emails exchanged and accessed by multiple parties. Prominent examples include board memos, commercially sensitive documents, such as product design documents, M&A (merger and acquisition) plans, financial reports, or customer information.

A content owner is empowered to revoke or change access rights at any time, or to set the expiration date so that once the content is no longer sensitive, access rights are relaxed or removed. The protection granularity is solution- and vendor-specific, and ranges from protecting a document library or a folder, a single file, to only protecting a confidential part of a file.

### Implementation observations and recommendations

Although EDRM offers effective data protection capabilities, it is a recent technology and its impact on the existing business processes needs to be carefully evaluated. For instance, there are some common pitfalls associated with EDRM, such as content over-protection, inappropriately blocked access or impact on e-discovery capabilities. To address these concerns, we advise our clients to take a structured and phased implementation approach. This includes a careful selection of use cases and identification of business benefits, proof-of-concept and pilot deployments, impact assessments and close involvement of business stakeholders. Furthermore, EDRM is not only about technology: having a robust governance structure, proper training and awareness of the user community are important success factors as well.

Finally, our experience shows that EDRM is most effective when combined with other data-centric protection technologies, such as DLP (Data Loss Prevention). EDRM and DLP have complementary capabilities, which can be leveraged to provide a more cohesive data protection architecture. For instance, a DLP solution is able to detect sensitive data and apply EDRM policy to restrict access to identified data.

If you would like to have an initial conversation about EDRM and Deloitte's approach to making it a success, please get in contact with our team.

**Dr. Dusko Karaklajic**
**Manager**
**Cyber Risk Services**
+41 58 279 7386
Email

### Privacy issues you need to be aware of this winter

Our summary of the November and December Privacy Flash editions provides an overview of the most important privacy developments of the past two months.

Two areas stand out this winter. Firstly, much anticipated guidance on the GDPR is slowly becoming available. Following the recently published GDPR guidance issued by both the UK and Belgium, the Hungarian DPA also published a guide for data controllers and data processors, explaining how to become compliant with the upcoming GDPR in 12 steps.  In the coming months, it is expected that DPAs will issue additional instruments and guidelines for further assisting companies and organisations in preparing for the GDPR. Also related to the GDPR, the Article 29 Working Party gave a comprehensive run-down of the various new GDPR concepts that were discussed during the so-called 'Fablab' workshop on 31 July, 2016. The purpose of this workshop, entitled "GDPR/from concepts to operational toolbox, DIY", had been to provide assistance on how to properly prepare for the GDPR on a timely basis.

Finally, the French CNIL published the results of their GDPR public consultation. Additional guidance, both from the UK ICO as well as the Article 29 Working Party, is expected over the coming weeks and months.

In the area of enforcement, a British telecommunications company was fined £400,000 for failing to meet its security obligations in terms of implementing foundational security measures. The company had done too little to protect the customers' information which had resulted in a major data breach. This fine is one of the biggest of the ICO ever and falls just below ICO's limit of £500,000.

The second major development relates to enforcement actions. The Dutch DPA has announced that it shall soon hand out fines following various investigations around data breaches with several companies. The DPA has further shared that it has received almost 4000 cases of data breaches including cases where the protection of personal data was considered "drastically insufficient". It is therefore to be expected that fines will follow in due course. German DPAs announced that they will start auditing around 500 companies on the topic of international data transfers with the goal of raising awareness. In France, a new act was published that makes class actions possible for violation of the French data protection legislation.

**In other key developments:**

- The Court of Justice of the European Union declares dynamic IP addresses to be personal data in Breyer decision.
- Last month, during her appearance before the Culture, Media and Sports Select Committee, UK Secretary of State Karen Bradley announced that the UK shall implement the GDPR in May 2018 regardless of the circumstances around Brexit. This aspiration has been widely approved, including by the ICO.
- The European Parliament gives green light to the EU-US data protection Umbrella Agreement.

**Dr. Klaus Julisch**
**Director**
**Cyber Risk Services**
+41 58 279 6231
Email

## Privacy Flash

For a detailed view of the latest privacy and data protection trends across Europe, download the PDF documents below:

- **Issue 9, Dec 2016**
- **Issue 8, Nov 2016**

# Events, conferences and contacts

### CPDP Computers, Privacy & Data Protection

Brussels, Belgium
25 – 27 Jan 2017
www.cpdpconferences.org

The annual Computers, Privacy & Data Protection (CPDP) conference brings together academics, lawyers, practitioners, policymakers, industry and civil society to discuss legal as well as technological developments in data protection and privacy.

### European Privacy Academy

Dolce La Hulpe, Belgium
www.europeanprivacyacademy.com

The European Privacy Academy is a unique training, knowledge and networking centre, focused on practical day-to-day management of privacy challenges. It provides both an on campus data protection officer course and on-campus or in-house department-specific data protection training.

These trainings allow attendees to learn how to efficiently manage privacy and security in an integrated risk-based manner.

**The next European Privacy Academy DPO Course sessions will take place on:**
08 - 11 May 2017 and 18 Sep 2017
13 - 16 Nov 2017 and 05 Feb 2018
07 - 10 May 2018 and 17 Sep 2018

### IAPP Europe Data Protection Intensive

London, United Kingdom
13 – 16 Mar 2017
www.iapp.org/conference/iapp-europe-data-protection-intensive/

The Data Protection Intensive of the International Association of Privacy Professionals (IAPP) returns to London from 13 to 16 March 2017 and offers data protection professionals from around the world the opportunity to deep dive into today's critical data privacy topics and the coming challenges. The intensive is divided into a two-day training and workshop taking place as from 13 to 14 March. These practical sessions are followed by the actual conference on 15 and 16 March.

### Cyber Risk Services contacts

For further information or an individual consultation on how our Cyber Risk experts can help you, please do not hesitate to contact us.

**Dr. Klaus Julisch**
**Director**
**Cyber Risk Services**
+41 58 279 6231
Email

**Mark Carter**
**Managing Partner**
Risk Advisory
+41 58 279 7380
Email

Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/ch/about for a detailed description of the legal structure of DTTL and its member firms.

Deloitte AG is a subsidiary of Deloitte LLP, the United Kingdom member firm of DTTL.

Deloitte AG is an audit firm recognised and supervised by the Federal Audit Oversight Authority (FAOA) and the Swiss Financial Market Supervisory Authority (FINMA).

This publication has been written in general terms and therefore cannot be relied on to cover specific situations; application of the principles set out will depend upon the particular circumstances involved and we recommend that you obtain professional advice before acting or refraining from acting on any of the contents of this publication. Deloitte AG would be pleased to advise readers on how to apply the principles set out in this publication to their specific circumstances. Deloitte AG accepts no duty of care or liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.