swisscom

Targeted Attacks

Cyber Security Report 2019

© February 2019
Swisscom (Switzerland) Ltd
Group Security
Alte Tiefenaustrasse 6
3048 Worblaufen
www.swisscom.ch

Table of Contents

Introduction

Swisscom's 2019 Cyber Security Report has been published. Based on the threat situation, which we have updated once again this year, we have taken a more detailed look at a topic that is currently of particular concern to the security community within Swisscom, to our partners and customers, but also internationally: APTs.

Advanced persistent threats (APTs) involve attackers with a large amount of resources attacking a clearly defined target to obtain specific information or cause lasting damage. To explain the relevance of this adversary type we have compared APTs to other threat actors such as cyber criminals, terrorists and hacktivists. What sets APTs apart from other actors?

Whereas criminals take the path of least resistance to generate as much profit as possible, both terrorists and hacktivists use attacks for publicity but have few resources and little know-how, APTs proceed much more subtly. The target is selected carefully and monitored over months or even years. Seemingly boundless resources are used to build up know-how and develop suitable tools. In addition, great care is taken to maintain the outmost secrecy, during and after the attack so that neither the attacker nor the target can be discovered too soon.

The report describes attackers' motivations and their resources. Based on data collected and evaluated by Swisscom, it shows which methods and tools attackers use most frequently. We will also highlight which countermeasures are particularly effective and which countermeasures offer the best detection capabilities.

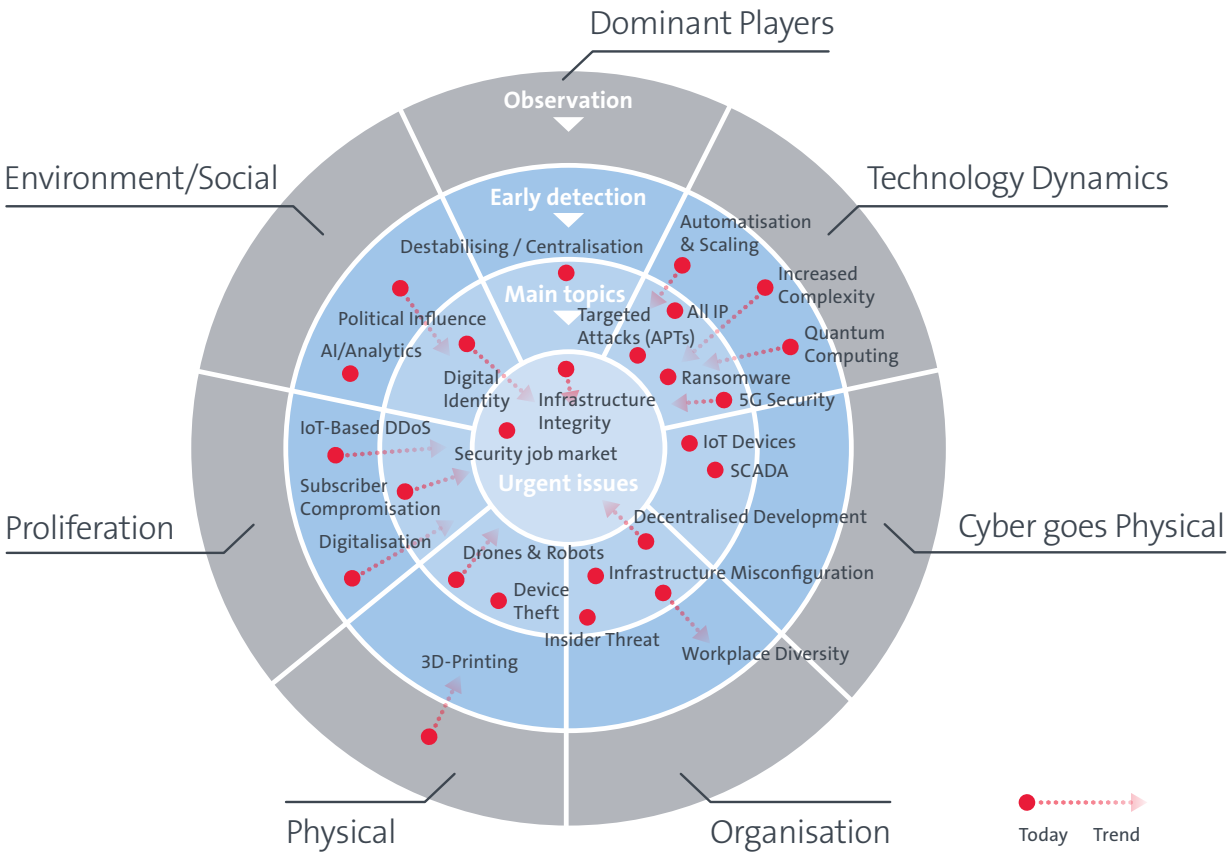
We are very pleased that we were able to win Costin Raiu from Kaspersky's GReAT for an introductory interview. Costin is a world-renowned expert in the field of APTs who was happy to share his knowledge with us.

This report is a joint work between different departments within Swisscom.

Status Report – Threat Radar

Threats arise out of the constant development of new technologies and their application and spread across society.

Potential threats must be detected at an early stage and documented systematically. To illustrate the threat situation and its evolution, we use the familiar radar to which we have already referred in previous publications of of Swisscom's Cyber Security Report.



Threat Radar

Methodology

The threat radar is broken down into seven segments that differentiate between the various threat domains. The threats belonging to each of these segments will be assigned to one of four concentric rings. These rings indicate a threat's actuality and thus also our estimation of probability in assessing such threats. The closer the threat is to the centre of the circle, the more relevant is the threat and more important is it, to take appropriate countermeasures.

We refer to the rings as:

- **Urgent issues:** Threats that are being executed wide spread and are binding large amounts of resources.
- **Main topics:** Threats that are detected still rarely and are countered with a normal deployment of resources. Often, defined processes already exist to efficiently defend against these threats.
- **Early detection:** Threats that have not yet been carried out or whose impact is currently very small. Projects have been launched with the goal of addressing the growing significance of these threats at an early stage.
- **Observation:** Threats that may occur in the next years. No concrete measures have been defined for handling these threats.

Moreover, the individual threats indicated by the aforementioned points show a trend which may be of increasing, decreasing or stable criticality. The length of the trend beam indicates how swiftly the threat's criticality is expected to change.

Threats

The following is a brief description of the seven segments of the threat radar.

Dominant Players

This segment covers threats arising through dependencies on dominant manufacturers, services or protocols.

Urgent issues	*Infrastructure Integrity:* Key components of critical infrastructure may have had vulnerabilities built into them, whether through negligence or maliciously, which endanger the security of the system.
Main topics	*Destabilising Centralisation:* Strong centralisation in the structure of the Internet leads to cluster risks. The breakdown of one service, e.g. Amazon Web Services (AWS), can have a global impact.

Technology Dynamics

This term covers threats arising from the fast pace of technological innovation, which both creates new threats itself and also offers attackers new avenues for attack.

Main topics	*Targeted Attacks:* Targeted and complex attacks designed to reach a specific goal. This threat type is explained in greater detail in later sections of this report. *All IP:* The nationwide rollout of All IP also increases the risks associated with VoIP technology. *5G Security:* 5G is still a young technology and its launch will not only offer many new opportunities but will also open the door to unknown threats. *Ransomware:* Large amounts of critical data are encrypted and only (possibly) decrypted in exchange for the payment of a ransom.
Early detection	*Automation & Scaling:* Greater automation of technical operations will mean that the repercussions of successful attacks and misconfigurations will be greater. *Increased Complexity:* The complexity of systems, especially across technological and corporate borders, is on the rise. This increases risk exposure and hampers troubleshooting. *Quantum Computing:* Quantum computers can render existing cryptographic methods useless because they can crack them in no time.

Cyber goes Physical

This term covers attacks on infrastructure conducted from cyberspace, which will increasingly cause damage in the physical world.

Main topics

IoT Devices: Devices with weak protection could be compromised or sabotaged. This could restrict their own functions, including their availability or data integrity.
SCADA: There are many technical control systems for critical infrastructure, which are poorly protected and not well maintained.

Organisation

Organisational threats arise through changes in the organisation or exploit weaknesses in an organisation.

Main topics

Infrastructure Misconfiguration: Exploitation of misconfigured infrastructure components and vulnerabilities that are identified too late and patched late.
Workplace Diversity: Aside from the many opportunities that new working models bring, an uncontrolled use of such models, e.g. "bring your own device" (BYOD) or the increased use of remote workplaces, exposes companies to greater risks.
Insider Threats: Partners or colleagues manipulate, misuse or sell information, either through negligence or for malicious intent.
Decentralised Development: Classic pure development departments disappear. Application development merges with the operations departments and move closer to the business units. Release cycles are getting shorter.

Physical

Threats that arise from the physical environment that are generally more focused on physical targets.

Main topics

Device Theft: The theft of devices – especially critical infrastructure components and, increasingly, IoT Devices – may result in a loss of data or impair service availability.
Drones and Robots: Reconnaissance and attacks over longer distances will become easier and cheaper.

Observation

3D Printing: Improvements in the quality of 3D printers will make it cheaper and easier to create e.g. keys and other physical devices.

Proliferation

Threats that benefit from ever easier and cheaper access to IT media and know-how are known as proliferation threats, because this creates new potential ways of attack: It also increases the availability of tools that can be used for attacks.

Main topics	*Subscriber Compromisation:* Malware attacks mobile users' private data or is used to attack telecommunication or IT infrastructure.
Early recognition	*IoT-Based DDoS:* Strong growth in the number of IoT Devices coupled with low-level protection creates more "takeover candidates" for botnets. *Digitalisation:* The growing interaction between the virtual and real world as also private and corporate environments create new ways of attacks.

Environmental/ Social

This covers threats that arise out of socio-political change or which are either facilitated or become more valuable to attackers.

Urgent issue	*Security job market:* Great difficulties of meeting the demand for security professionals mean that not enough expertise is available to counter the increasingly complex and intelligent attacks.
Main topics	*Digital Identity:* Trusted personal digital identities may be misused or stolen, e.g. to conclude contracts under the names of others.
Early detection	*AI/Analytics:* More data and better analytical models provided by AI can be misused to influence people's behaviour. Decisions are increasingly left to autonomous systems. *Political Influence:* Political trends can influence technological or economic decisions, e.g. in the selection of technology suppliers. This can create new risks.

Conclusion

The threat situation remains complex. Attackers are profiting from the increasing value of virtual assets, which thus further motivates them to launch a targeted attack. In addition, technological innovations and the convergence of the physical and virtual worlds are creating new opportunities for attacks. However, it also shows that no specific threat is developing, but rather that threats are subject to fluctuations and trends.

Compared to last year's picture, we can say that the threat situation has remained stable. Although some threats, such as *Infrastructure Misconfiguration* and *Workplace Diversity,* have declined this year, most still exist and are changing only minimally.

For both declining threats, we attribute the "relief" not to falling interest by potential attackers, but rather to the increased maturity of the affected infrastructures. Workplace diversity, for example, is actively being managed at more and more companies, mobile device management (MDM) tools are being used and directives for the use of "bring your own device" (BYOD) are being developed and implemented.

Threats via *SCADA* (industrial control) systems and *IoT* (Internet of Things) Devices remain in the main focus, but we do not see any short-term changes. IoT penetration is not yet high enough to further exacerbate the threat situation.

Drones, on the other hand, are currently becoming more widespread, with the associated negative consequences, some of which have also been reported in the media. For this reason, we currently see a strong trend towards a worsening threat situation.

The threat situation remains complex. Attackers are profiting from the increasing value of virtual assets, which thus further motivates them to launch a targeted attack.

Interview Costin Raiu

(Kaspersky GReAT)

We were given the opportunity to ask Costin Raiu six questions about APTs and to benefit from his experiences and observations as an expert on the subject.

1. Costin Raiu, what are the primary characteristics that make up an Advanced Persistent Threat (APT)?

In our opinion, this is what makes a malware or attack advanced:

- the *usage of a zero-day exploit* as seen with Sofacy, also known as APT28, Pawn Storm or FancyBear. This is probably a champion among all when it comes to the number of discovered zero-days.
- a *highly complex, modular platform* to carry out various functions such as Regin and ProjectSauron.
- The *usage of sophisticated techniques for infection, persistence or exfiltration.* For instance, RedOctober used a very clever persistence mechanism in the form of an Office and Adobe Reader plugin, which has the ability to execute code hidden in specially constructed documents; this also includes various bootkit techniques.

Other characteristics are *Slow replication,* coupled with network *level persistence, Infection of pro-level network hardware* such as core routers and *supply chain attacks.*

Good examples of how those attacks have been performed are Duqu2, SYNful Knock or Shadowpad and CCleaner compromise.

This list is non-conclusive. Other examples are attacks on hardware features, infection of the BIOS, destructive attacks against hardware with Stuxnet as a prominent example or multi-platform malware.

2. What are the most significant changes in APT activity that you are observing and what areas are primarily affected by these changes?

We are tracking over 100 APT groups and operations at the moment. We started tracking APT groups on a regular basis in 2010, after the story of Stuxnet, and when it became clear this was a trend, we decided to continue. Since we reached knowledge about 100 APT groups and operations in 2015, around the same time we launched our private APT reporting service.

We also observe more and more APT groups engaging in fileless attacks. This makes it more difficult to detect infections, as no malicious files can be found in the system. Additionally, we are seeing an increasing number of groups adopting public tools such as Empire Powershell, Metasploit, Cobalt Strike or Mimikatz. It makes it difficult to distinguish between them.

3. What was the most interesting APT that you have analysed?

Probably Duqu2. First of all, we thought Duqu2 was special because it was used to target Kaspersky Lab. The idea of an APT targeting a security company is a pretty bold one, because it's impossible to assume the intrusion will not be detected. Secondly, Duqu2 was rather special in the sense it was a memory-only threat, which, while running, existed only in the memory of several computer systems, without artifacts on disks. This complicated its detection a lot. Finally, the usage of a zero day in Windows to bypass Kaspersky products seemed quite interesting and resulted in several product improvements to detect such behavior in the future.

4. What are typical mistakes organisations do in order to be prepared for an APT attack and how they respond to an APT?

Most organisations focus on preventing an external attacker from getting access to internal resources, but few take measures to detect an attacker once he/she has access to the internal network. As I know from our research, attackers spend most of their time with lateral movement and exfiltration. So the organisations should focus on this phases. Also, lack to implement the Australian DSD TOP35[1] mitigation measures against APTs.

[1] https://acsc.gov.au/infosec/top-mitigations/mitigations-2017-table.htm

5. What are the typical mistakes attackers do during their operations? Where do you see organisations getting an advantage over their adversaries?

Often, we recognise Opsec mistakes such as VPN fails, forgotten PDB paths in binaries or compilation timestamps.

6. What are the most important capabilities to have to be prepared for APT large-scale intrusions?

For companies, it is essential to have access to private threat intelligence, having a fully operational Security Operation Center, implementing network filtering and a detection of lateral movement and exfiltration mechanism. Also, organisations should know and deeply understand how attackers work. For example, which tools they use and how they operate during the attack phases. Most of them use Mimikatz, Powershell and Webshells.

About Costin Raiu

Costin Raiu specialises in the analysis of advanced persistent threats (APTs) and complex malware attacks. He leads the Global Research and Analysis Team (GReAT) at Kaspersky, which investigated the Stuxnet, Duqu, Flame and EquationGroup operations, among others. Costin has more than 19 years' experience in antivirus technology and security research. He is a member of the Virus Bulletin Technical Advisory Board, a member of the Computer AntiVirus Researchers' Organisation (CARO) and a reporter for the Wildlist Organisation International. Prior to joining Kaspersky Lab, Costin worked for GeCad as chief researcher and was a data security expert for the RAV antivirus development group.

Components of Targeted Attacks

Depending on the threat actor, the mission or strategic goal of an attack will have completely different intentions, and threat actors have a wide range of ways to put them into practice.

The media often report that companies have been infected with a specific type of malware or that a specific type of malware has been used to steal a company's data. To understand targeted attacks, we must be aware that it is not the malware that is carrying out the attacks, but that businesses are being attacked by people. These are often referred to in the cyber community as threat actors or cyber operators and are the main component behind such attacks. The threat actors behind targeted attacks do not carry out these attacks indiscriminately, but have a strategic goal, a wide variety of motivations and diversified approaches, which serve as additional components of a targeted attack and are detected as it progresses.

The Threat Actor Landscape

Depending on the threat actor, the mission or strategic goal of an attack will have completely different intentions, and threat actors have a wide range of ways to put them into practice. For better orientation and to assess the potential and motivation of different threat actors, we divide them into the following groups:

Targeted attacks by advanced persistent threats

Advanced Persistent Threats (APTs) constitute the top tier of cyber threat actors. Targeted attacks by an APT are conducted based on a mission that aims to gain a strategic advantage in order to achieve political ends or positively influence technology developments. In this context, an APT is assumed to be a government or an entity that acts on a government's behalf. The special feature of an APT is that the attacks associated with it are considered "state-sponsored," which explicitly means that the threat actors are condoned by the state and thus represent "legal" (or at least state-protected) hackers. State legality, difficult traceability and relatively risk-free implementation have led more and more states to expand their cyber capabilities and APT attacks.[2]

[2] https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf

In addition to such "legal" APTs, there is another fringe group that can be seen as pioneers of states/governments that have not yet developed the capabilities to carry out advanced attacks such as those of an APT themselves. At the latest since the hacking team revelations of hacktivist Phineas Phisher, it has become clear that this fringe group pursues clear financial and strategic goals.[3]

Targeted attacks by cybercriminals

Cybercriminals are primarily opportunistic and use all of their available capabilities (e.g. a published exploitation of a Microsoft Office vulnerability) against a wide range of targets. Whenever they receive a capability, they use it against many opportunistic targets to profit from as many attacks as possible. In addition to opportunistic attacks, there are also targeted and well-organised cyber criminal attacks that aim at stealing large amounts of data or other assets from a defined target through a single attack and turn this into money. For this attack, the actors typically need to spend a significant amount of time inside of the target network. Such organised criminals are often just as technically skilled as many APTs. However, the decisive difference lies in the threat actors' strategic objectives.

Targeted attacks by terrorists

Whereas fear is widespread among the general public that terrorists will attack critical systems, not a single case has been reported thus far in which terrorists have pursued and achieved their strategic goals through targeted cyberattacks. In fact, the Cambridge Centre for Risk Studies knows of no non-state terrorist group that has developed the ability to carry out advanced, targeted cyberattacks which could cause physical damage.[4] At the same time, the 2018 Worldwide Threat Assessment by the US intelligence community concludes that terrorists primarily use cyberspace for media purposes.[5]

We still assume that cyber terrorism remains a threat and will play a greater role in the future.

Targeted attacks by hacktivists

Hacktivists typically carry out targeted attacks for political motives as a form of protest. They congregate globally in groups of like-minded individuals in order to coordinate and carry out attacks. Alternatively, they may carry out attacks on their own. The skills of hacktivists vary greatly. The aim is to reach the chosen strategic goal as quickly as possible and attract a lot of media attention. So far, it has been noted that these threat actors primarily perform smash-and-grab operations in order to publicise their success as quickly as possible.

[3] https://arstechnica.com/information-technology/2016/04/how-hacking-team-got-hacked-phineas-phisher/
[4] https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/risk/downloads/180620-slides-evan.pdf
[5] https://www.wilsoncenter.org/article/world-wide-threat-assessment

Targeting

The targets of targeted attacks are not chosen randomly, but based on the specific relationship between the target and the adversary.

Targets of Interest

The more a target satisfies the needs of an adversary the more it becomes a Target of Interest (TOI). The primary aspects describing a TOI are the unique ability to satisfy the need of the adversary, the required effort and cost associated with conducting the attack, as well as the risks it may pose to the attackers.

Targets of Opportunity

A Target of Opportunity (TOO) is of secondary importance. Such targets meet a threat actor's subordinate needs and might be attacked as a bridge to the actual Target of Interest. However, it is also possible that the target was compromised because it was vulnerable to a particular exploit at a specific moment in time. The Target of Opportunity can also become the Target of Interest if the threat actors later discover that the victim is of higher value than initially concluded.

The more a target satisfies the needs of an adversary the more it becomes a Target of Interest (TOI).

[6] www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf

Conducting the Attack

There are many ways to describe a cyberattack. We have chosen the MITRE ATT&CK framework, which is based on data from attacks that have been observed in real world intrusions. ATT&CK is similar to the cyber kill chain[7] method for describing cyberattacks[8]. Whereas the cyber kill chain provides more of a helicopter perspective, the ATT&CK framework details the activities of more than 80 threat actors (groups). ATT&CK primarily contains the activities of advanced persistent threats in the different attack phases, described on the basis of the tactics, techniques and procedures (TTPs)[9] of these threat actors.

Our analysis of the data was carried out over a period of several weeks via ATT&CK Enterprise[10] (hereinafter referred to as "ATT&CK"), the last access being in January 2019. ATT&CK is continuously extended and updated. However, the data gathered by the framework and the experiences of Costin Raiu's GReAT team enable us to do very precise evaluations in terms of quality and quantity.

In January 2019, ATT&CK included

The following sections describe what we believe are the most important high-level findings from the ATT&CK framework, with a clear focus on Advanced Persistent Threats.

[7] https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
[8] https://www.mitre.org/publications/technical-papers/mitre-attack-design-and-philosophy
[9] https://apps.dtic.mil/dtic/tr/fulltext/u2/1004650.pdf
[10] https://attack.mitre.org/matrices/enterprise/

The Attack Phases

ATT&CK considers tactics to be the different stages of an attack that a threat actor works through to achieve his strategic goal. In this context, we also speak of tactical goals. ATT&CK defines the following tactics:

Initial Access	The initial access phase is the starting point for all the subsequent phases of an attack. It includes the initial contact with the attack target and compromising the so-called "patient zero."
Persistence	Persistence points within the target network ensure ongoing access to the compromised network. The more important the target is to the adversary, the more effort is put into persistence points for long-time access to the network.
Privilege Escalation	The escalation of privileges is often needed to install malware or persistence points. Increased privileges are sometimes also required to be able to spread to other systems or gain access to the strategic goals (e.g. data).
Discovery	Exploration within the target network is required to locate systems, users and data relevant to the mission.
Lateral Movement	This refers to moving across a network to the relevant data for the mission. This is often accompanied by the execution phase and the installation of further persistence points.
Collection	The relevant data is collected.
Exfiltration	This is the final phase required to successfully complete the mission and involves exfiltrating the relevant data.

The following phases run in parallel to these phases, depending on the successful achievement of the objectives of the respective phases:

Execution

The execution of malicious code on a local or remote system primarily takes place in the initial access and lateral movement phases. The next phase cannot be reached without execution of code controlled by the attacker. Execution is thus one of the most important prerequisites for the further development of the attack and for spreading across the target network.

Defense Evasion

Bypassing defense and detection mechanisms, e.g. by turning off the firewall at the endpoint or deleting log data, is one of the tactical goals that threat actors use in every other phase of their mission to either conceal their presence or bypass detection mechanisms.

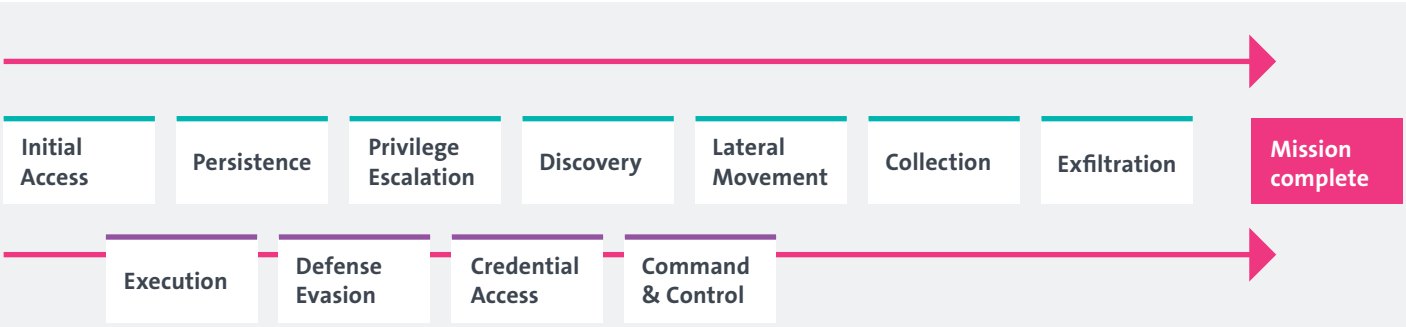
Credential Access

Valid credentials play a key role for attackers. Firstly, it enables access to systems with legitimate credentials and lateral movement within the target network. Secondly, it grants access to the data that the attackers want. Furthermore, reusing credentials enables attackers to conduct an attack using few resources because no exploits have to be written, acquired or employed in any other way.

Command & Control

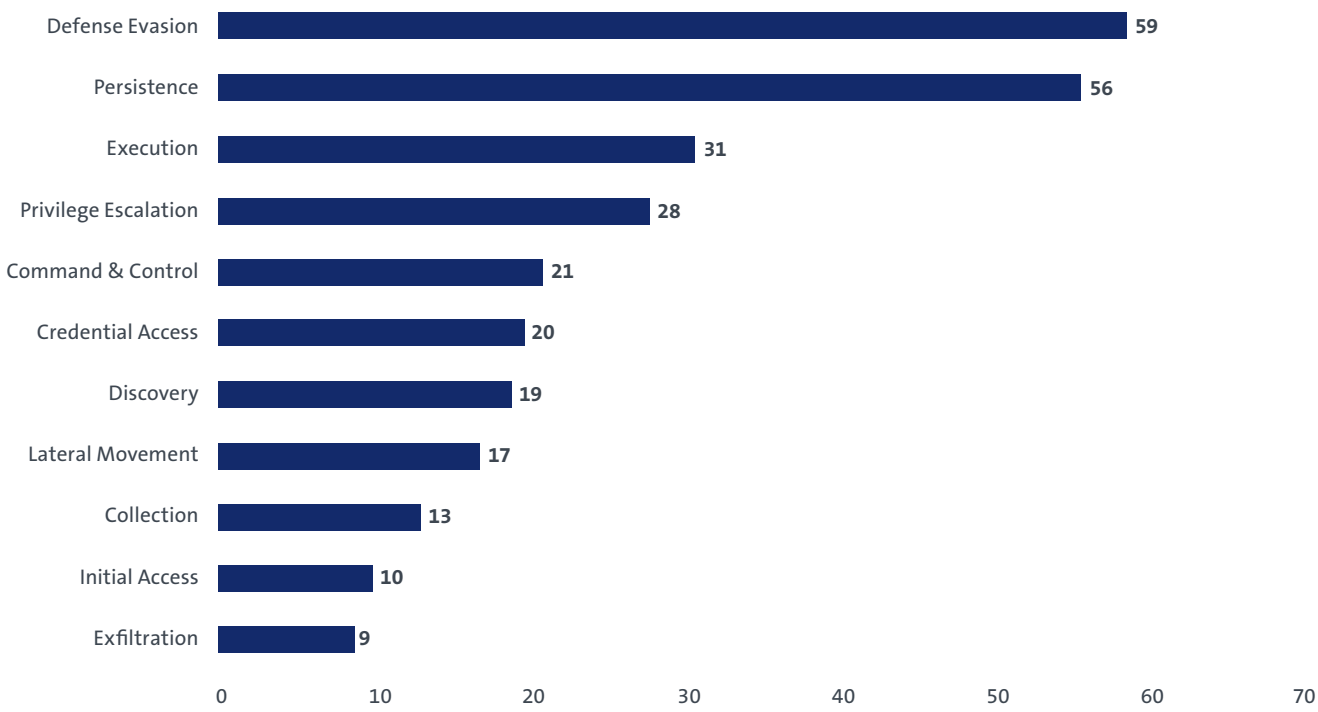
The command & control channel is the attacker's means of communication to keep the compromised target infrastructure under his control. If the attacker loses this channel, the attack is literally stopped. As such attackers often establish multiple command & control channels to ensure access.

The following illustration shows the connections:



Threat Actors' Techniques

In order to reach or complete a specific phase, the threat actors in the ATT&CK framework[11] use a wide variety of techniques. Each phase can contain several techniques and each technique can be used within more than one phase. ATT&CK contains 224 of these techniques, which are found in the various phases as follows:



The bar chart provides important insight into the modus operandi of threat actors and clearly shows the phases in which they posses the most capabilities. Looking at the phases in terms of the number of techniques present, the analysis shows that threat actors have access to a very broad range of approaches for outsmarting defense mechanisms in the different phases of the attack through defense evasion, and just as many approaches available to guarantee them long-term access in the persistence phase.

Extract from the interview with Costin Raiu, which also clarifies this statement:

What are the most important capabilities to have to be prepared for APT large-scale intrusions?

Organisations should know and deeply understand how attackers work.

For example, which tools they use (most of them use Mimikatz, Powershell, Webshells) and how they operate during the attack phases.

[11] https://attack.mitre.org/

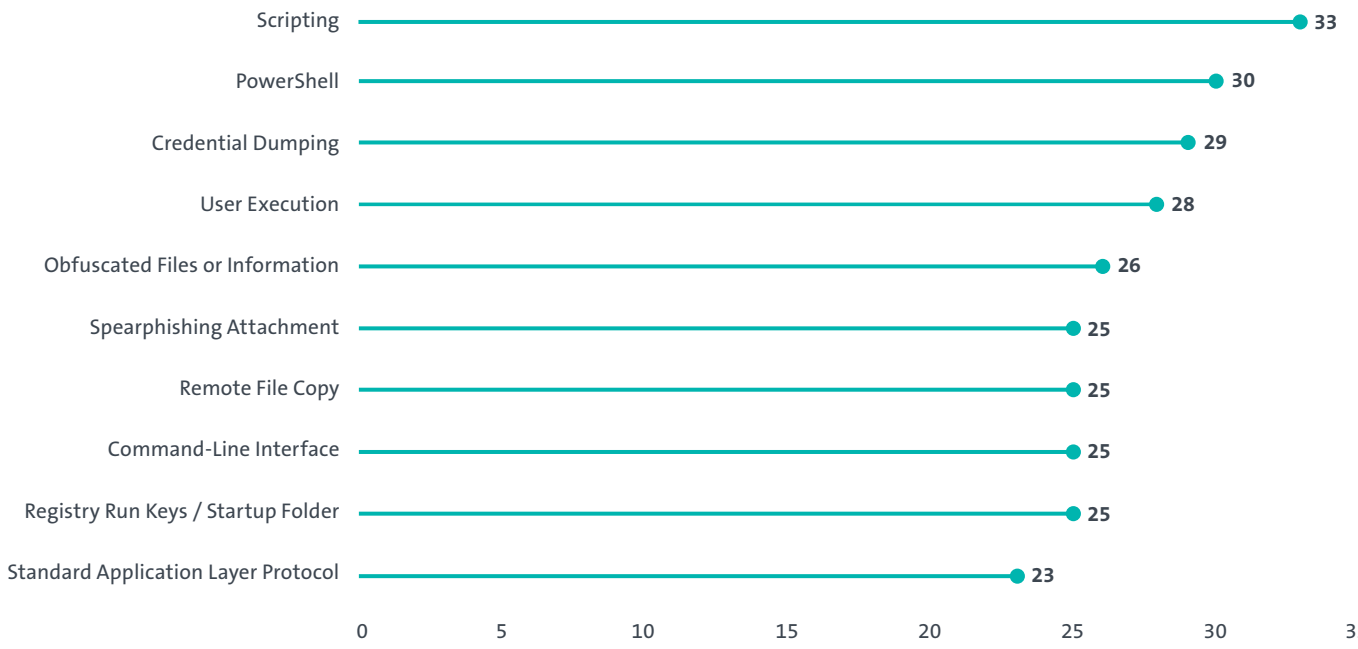
What are the most significant changes in APT activity that you are observing and what areas are primarily affected by these changes?

We observe more and more APT groups engaging in fileless attacks.

This makes it more difficult to detect infections, as no malicious files can be found in the system.

Most-used techniques by threat actor
An evaluation of the APT groups and their techniques shows a clear trend towards file-less attacks. This was also confirmed by Costin Raiu.

The following illustration shows the ten most frequently used techniques across the 80 threat actors within ATT&CK:



The top ten approaches can be summarised under two themes: “Living off the land” and “Proven methods still work”.

Living off the land	More and more APT groups are relying on scripting languages that are now integrated as standard in Windows operating systems, such as PowerShell and command-line interfaces, to execute their malicious code without being detected by application whitelisting solutions or leaving significant traces on the system.
	Registry run keys and entries in the Windows start-up folder remain the most popular persistence mechanism technique among threat actors.
Proven methods still work	Not all threat actors have the resources to develop zero-day exploits. Most of them continue to rely on spear phishing attachments and user execution to dupe users into executing malicious code.
	APT threat actors use simple ways to achieve their goals. Through Credential Dumping adversaries obtain valid credentials and use them to move laterally inside of the target network and ensure long-term access.
	To disguise their code, attackers still rely on Encodings and Encryptions and do use common protocols like HTTP or DNS to blend into normal traffic where the majority is using remote file copy methods to transfer their malicious software.

Threat Actors’ Software

Software implements techniques required by threat actors to successfully run through a specific tactic. For this, they use a wide variety of software categories that represent either a tool, utility or malware within ATT&CK.[12]

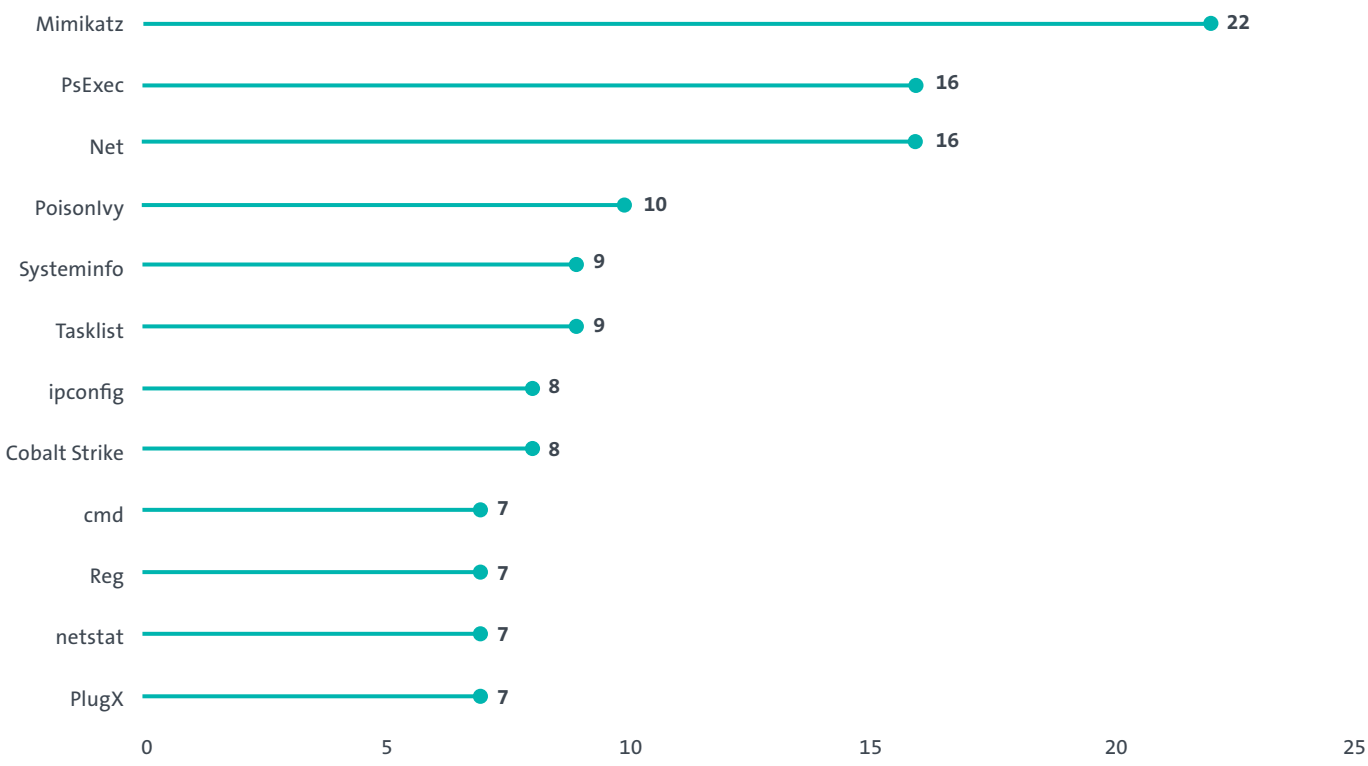
[12] https://www.mitre.org/sites/default/files/publications/pr-18-0944-11-mitre-attack-design-and-philosophy.pdf

Most-used software by threat actor type
An analysis of the APT groups and the software they use shows that off-the-shelf tools and software already provided by the operating system are used most frequently. This observation matches Costin Raiu's experience.

The following illustration shows the ten most frequently used software types across the 80 threat actors within ATT&CK:

What are the most significant changes in APT activity that you are observing and what areas are primarily affected by these changes?

We are seeing more and more groups adopting public tools such as Empire Powershell, Metasploit, Cobalt Strike, Mimikatz, making it difficult to distinguish between them.



Countermeasures and their Effects

Countermeasures against targeted attacks build on standard protection based on preventive measures such as applying current patches, implementing two-factor authentication, connection to the internet only through a proxy etc. These measures are sometimes sufficient to redirect the interest of non-state threat actors towards other targets.

In the previous sections, we looked at the basic aspects of threat actors, which are reflected in their intent (strategic goals), opportunity (attack surface) and capability (techniques). These aspects must be taken into account when developing appropriate, effective countermeasures. Probably the most effective defence would be to eliminate the strategic goal (intent). Governments or companies that do not store data are not targeted by governmental threat actors who are engaging in espionage and want to benefit from stolen data. However, this defence can only be employed rarely. If we look at the available attack surface, it has increased rather than decreased in size in recent years. Increasing digitalisation, the storage of data in the cloud and everything-connected, always-on or IoT Devices are presenting an exorbitantly large attack surface for companies, society and individuals.

We must therefore base our countermeasures on threat actors' capabilities and techniques, which often ends in a head-to-head race and, given the many approaches available, this appears extremely complex at first glance.

However, on closer inspection, it's clear that most techniques and the employed software can be identified using detection methods that track system activity.

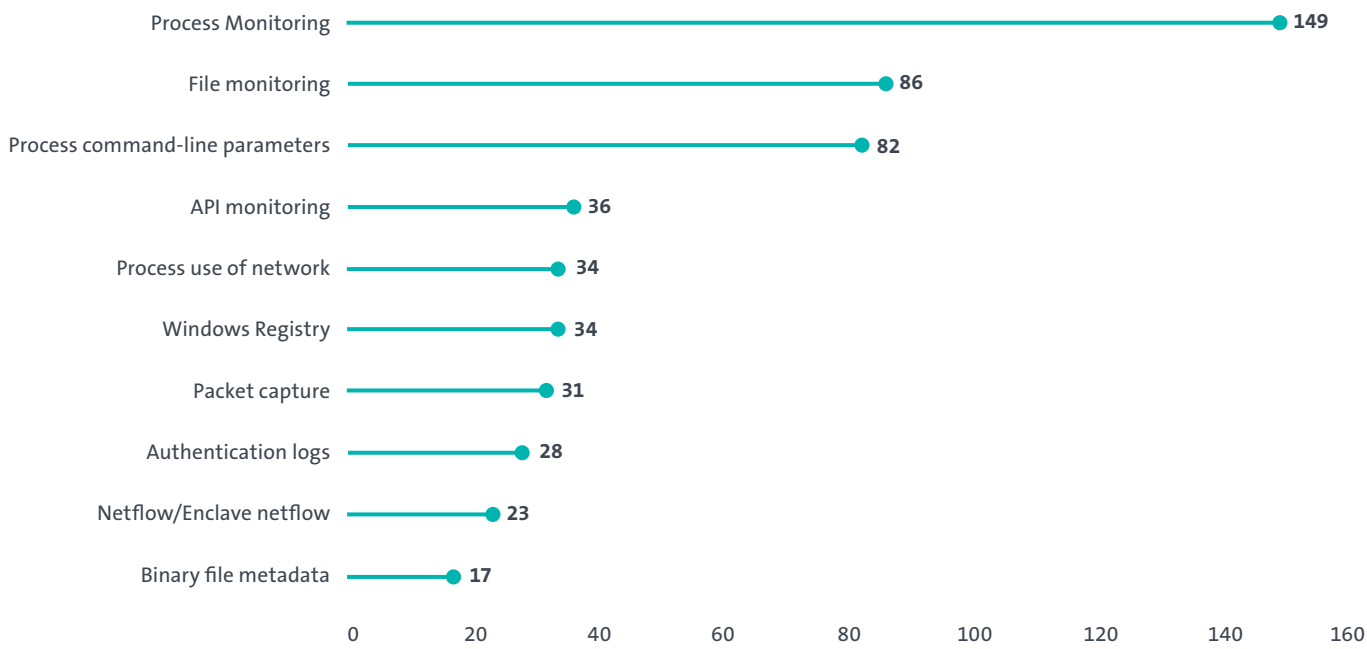
The Detection Methods with the most Coverage

Our analysis shows that a majority of the procedures of threat actors can be detected by monitoring process and file operations. These detection methods are the most effective ones, to detect the attack patterns used within targeted attacks. This, too, tallies with what Costin Raiu said.

The following illustration of the top ten detection methods underlines this once again:

What are typical mistakes organisations do in order to be prepared for an APT attack and how they respond to an APT?

Most organisations focus on preventing an external attacker from getting access to internal resources, but few take measures to detect an attacker once he/she has access to the internal network.



Detection methods for process activities identify the majority of the existing procedures of threat actors. User and network activity provide further context.

System activity	The execution of code controlled by threat actors is a prerequisite for achieving their strategic goals. Monitoring processes, files and changes in the Windows registry is the most effective detection method for tracing a threat actor's intrusion pattern. Even though this form of detection brings the greatest added value, very high data volumes and efforts for tuning are to be expected. Processes, network connections, file and registry operations must be fully understood.
User and network activity	In addition to monitoring system activity, network data and user authentication logs provide additional insight into the adversaries intrusion pattern.

What is Swisscom doing?

Targeted attacks are becoming increasingly likely and the currently available technological measures are often insufficient for keeping pace with the abilities of professional cyber threat actors. For these reasons, Swisscom relies on a risk-based security model that requires a high level of security awareness within the organisation by employee training and involves the community in the security culture, e.g. through the Bug Bounty Programme[13], and fundamental preventive security measures e.g. whitelisting and the patching of applications and restricting of network traffic and e-mail attachments. Prevention is one important aspect, however this might ultimately fail when faced by highly motivated threat actors. It is therefore necessary to be proactive, understand threat actors' tactics, techniques and procedures and incorporate any gained insight into the detection process. We recommend simulating a targeted attack through red teaming exercises, conducting threat hunting and engage in sharing groups.

Red teaming

Because attackers are always one step ahead, we have become attackers ourselves. In 2015, Swisscom decided to break new ground by becoming the first Swiss company to establish an official red team. The red team consists of a small group of Swisscom employees who carry out realistic attacks against Swisscom infrastructure and services. These are so called ethical hackers, i.e. hackers with good intentions who conduct targeted attacks against Swisscom, though NOT against client applications or client data.

What are their goals?

- To identify vulnerabilities and their impact before others do;
- To test the blue team and thus help the company develop countermeasures and improve processes;
- To learn from incidents at other companies and test whether they could occur also at Swisscom.

Targeted attacks are becoming increasingly likely and the currently available technological measures are often insufficient for keeping pace with the abilities of professional cyber threat actors.

[13] https://www.swisscom.ch/en/about/company/portrait/network/security/bug-bounty.html

Threat hunting

Threat hunting aims to detect previously undetected threats. It is not a replacement for a functioning Security Operations Center (SOC), but uses partly automated, and even manual methods for detecting attack behaviour and patterns that could not be detected by existing security mechanisms. This approach supplies new detection methods, for example. Swisscom CSIRT regularly conducts threat-hunting sessions to identify threats within the Swisscom network. As part of this, the ATT&CK Framework often serves as a reference to understand the tactics and techniques of the different threat actors. In this context, CSIRT regularly publishes new detection methods for SIGMA[14] and YARA[15] and makes them accessible to the community. SIGMA is a generic and open signature format with which relevant detection log data can be described once and which can be used for a variety of SIEM and log systems. SIGMA is one of the few tools that can describe attacks with ATT&CK tactics and techniques and makes detection directly useful for others. YARA enables you to create your own signatures and detection methods that can then be used for both files and memory scans. Swisscom CSIRT regularly creates YARA rules for attacker toolsets and shares these with public communities such as Florian Roth's[16] signature base and other closed communities.

As mentioned in the previous sections, we must accept that attacks are carried out by people and not by systems. Thererfore also people are needed to react to them. Swisscom operates multiple Security Operations Center (SOC) to be able to investigate possible activity by attackers in a systematic way. Swisscom CSIRT analysts become active as soon as activity is detected which points to more targeted attacks on Swisscom's IT infrastructure.

Sharing groups and communities

In addition to sharing detected attacks based on SIGMA and YARA, Swisscom CSIRT and its staff are active members of many trust groups for operational cooperation in the daily work of CSIRTs, SOCs and threat intelligence teams. These trust groups are designed to bring together people with similar problems in their everyday work and to simplify the exchange between them. Swisscom regularly provides these sharing groups and communities with information on current observations, risks and indicators of malware and attacks.

Comprehensive corporate protection thanks to early detection of and professional intervention in cybersecurity attacks – available as a service

Today, vast volumes of corporate and personal information are available on various data sources (networks, applications, end devices, social media, the cloud, darknet, etc.). As networking and digitalisation continue to grow, so has the complexity of the threats. Timely detection of security-related incidents is essential.

Professional threat detection & response requires specific processes, tools, many years' experience and highly specialised employees. It is therefore almost impossible for individual companies to understand the constantly changing cybersecurity attacks and react accordingly. Support is thus required from experienced partners. Swisscom has been successfully protecting its network infrastructure, customer and product data as well as itself against cyber threats for years. It uses this

[14] https://github.com/Neo23x0/sigma/

[15] https://yara.readthedocs.org

[16] https://github.com/Neo23x0/signature-base

experience to minimise cyber risks in collaboration with its customers. Good data visualisation facilitates the early detection of potential security incidents. Timely analysis and appropriate reaction to a security incident improves the security level and the use of resources within the company.

Our Threat Detection & Response service enables corporate customers to choose between four service variants depending on how much cybersecurity support they would like from Swisscom. Here is a short overview:

Security Analytics as a Service: A dashboard provides the customer with an overview of potential security incidents from defined log data of the company.

Security Operation Center (SOC) as a Service: In addition to security analytics, customers receive analyses and concrete recommendations for action as well as direct access to specialists at Swisscom's SOC. We have been providing SOC services to Swiss companies both at home and abroad for more than ten years. Our SOC analysts can interpret security events and incidents competently and quickly.

Computer Security Incident Response Team (CSIRT) as a Service: Swisscom experts can be called on to analyse and tackle critical security incidents and lead the security incident management process. These experienced experts help customers preserve evidence and communicate with their customers and partners.

Threat Intelligence as a Service: Customers are informed proactively about the appearance of sensitive business and personal information of their company in public and closed networks (e.g. the darknet).[17]

Conclusion

In most cases, targeted attacks – especially those by APTs with strategic governmental goals – cannot be prevented. The increasingly digitised world is attracting more and more threat actors into cyberspace. We must therefore accept the growing likelihood that we will become a target of interest or at least a target of opportunity at some point in time. Threat actors have a variety of approaches at their disposal in the different phases of an attack, for which they are increasingly employing off-the-shelf tools and living-off-the-land methods. Although APTs belong to the top tier of cyber threat actors, they do not develop zero-day exploits for every operation. Rather, they use tried and tested methods in which people remain an attractive target in order to bypass security mechanisms and activate malicious code.

It is often claimed that attackers only need to succeed once to get into a system. Our analysis shows that we can make the opposite argument; namely that if we develop our detection measures in such a way that the approaches of threat actors can be detected, they need make only one mistake in order to be recognised. Focussing on detecting execution – the execution phase – is a promising approach here. However, with APTs in particular, the complete intrusion pattern should be understood before the attack is stopped.

[17] Further information and contact details: www.swisscom.ch/detection

Swisscom (Switzerland) Ltd 3000 Berne