CENTRE FOR
CYBER SECURITY

THREAT ASSESSMENT

Hackers leverage legitimate programmes in cyber attacks

FEBRUARY 2020

Content

Hackers leverage legitimate programmes in cyber attacks 3

Key assessment 3

Analysis 4

Cyber attacks of this kind are generally difficult to detect 5

Attacks that leverage victims' programmes are more frequent 6

Windows software is often leveraged in cyber attacks 7

Pentest-tools also use the attack technique 8

Advisory 10

Segmentation of the network 11

CENTRE FOR
CYBER SECURITY

Kastellet 30
2100 København Ø
Phone: + 45 3332 5580
Email: cfcs@cfcs.dk

1st edition February 2020.

Hackers leverage legitimate programmes in cyber attacks

The purpose of this threat assessment is to brief about an attack technique which is part of the cyber threat against Danish authorities and companies. The threat assessment is intended for authorities and companies as a means to highlight the attack type and provide information on how to defend oneself from it. The threat assessment is primarily intended for it-technicians and it-management.

Key assessment

- Hackers often use an attack technique against Danish and foreign public authorities and private companies that enable them to leverage the victims' own programmes for cyber attacks.
- The attack technique is difficult to detect and requires a proactive and holistic cyber security defence.
- Both foreign states and cyber criminals use this attack technique as a supplement to or instead of malware.
- Hackers often leverage pre-installed software in Windows such as PowerShell in this type of cyber attacks.
- Hackers can relatively easily use the attack technique, because the technique has been integrated in numerous so-called pentest-tools, which are publicly available online.

Analysis

Hackers with harmful intentions often use an attack technique against Danish and foreign companies and public authorities where they leverage the victims' own programmes to launch cyber attacks. Own programmes refer to programmes which are either pre-installed with the operating system or legitimate programmes installed by the victim. This attack technique is also known as "living off the land", because hackers essentially live off the tools which are available on the victim's system. The attack technique is not new, but is being used more frequently and is evolving.

The technique is effective and can be used by hackers to achieve the same goals as when they use malware.

The method is used both in connection with cyber espionage and cyber crime, and there are numerous international examples of this type of attack in recent years, including in Denmark.

The Danish Defence Intelligence Service's Centre for Cyber Security (CFCS) does not set a threat level for this attack technique. The CFCS prepare assessments and provide threat levels based on analyses of the actor's intention and capabilities. The purpose of a cyber attack may be to conduct espionage, cyber crime, cyber activism or cyber terrorism. The CFCS has set national threat levels and for a range of sectors that are critical to the functioning of the Danish society. These national levels are available on CFCS's website.

Post-exploit method

This threat assessment focuses on how hackers leverage the victim's legitimate programmes in order to achieve their goals after they have compromised the victim's system. This is often referred to as post-exploit. In relation to the Cyber Kill Chain®-model, this method is primarily related to Delivery and Exploitation, Installation and Command & Control. The difference steps of the model can be seen on Lockheed Martin's homepage or in appendix 1. Post-exploit includes activities used by the hackers to obtain administrator privileges or methods in a bid to exfiltrate data from the victim.

Hackers may also leverage legitimate programmes for initial compromise of their victims' systems, for instance, by using Macros. These methods are not included in this threat assessment, as the report only focuses on post-exploit techniques.

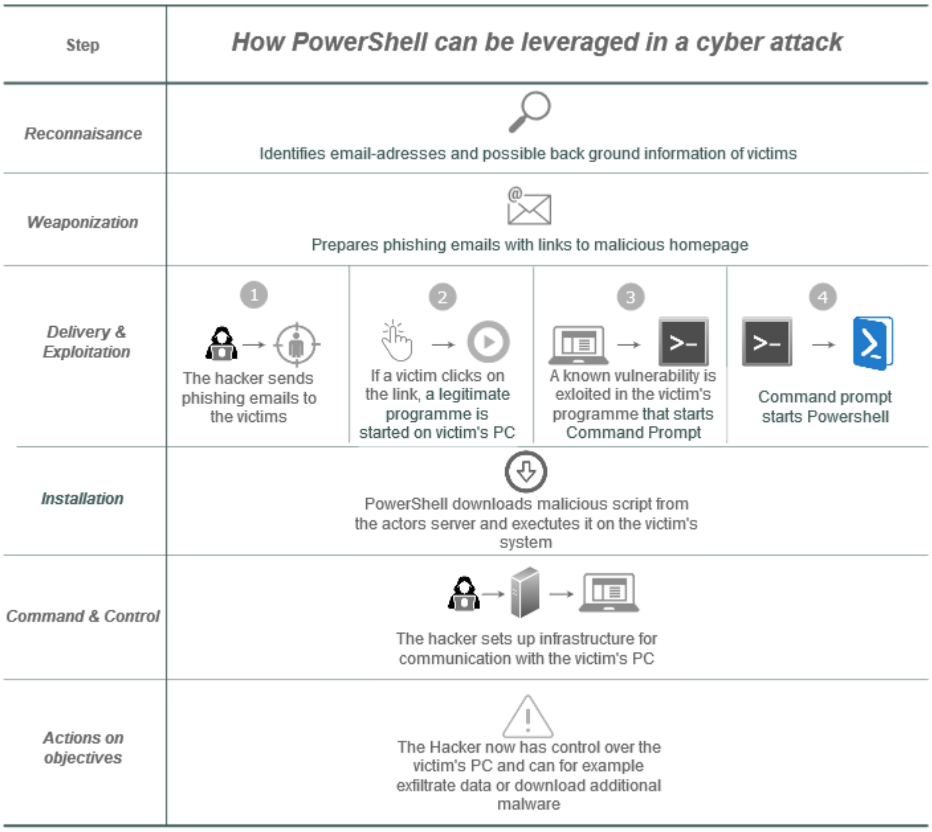
Cyber attacks of this kind are generally difficult to detect

This attack technique is particularly problematic as it is difficult to detect. Given that hackers leverage legitimate programmes that are pre-installed on the victim's system, the malicious activity is often not detected by regular antivirus programmes with companies and public authorities.

Also, these attacks are difficult to detect, because they are often fileless. Hackers do not use their own executable files to execute malicious code in fileless attacks, but instead leverage executable files already present on the victim's machine to execute their malicious code. Consequently, the malicious activity is only present in the memory of the system and not on the hard disk.

It is particularly in relation to this that attack technique differ from more traditional cyber attacks with malware. In cyber attacks with malware the actors install malicious files on the victim's system, which must subsequently be executed. When actors instead leverage the victim's programmes, there are no external executable files in this stage of the attack. Leverage of the victim's own programmes may also be conducted in combination with malware. Actors can gain relevant access in a network via the victim's own programmes in order to shut down the victim's antivirus and subsequently, hackers can install malware such as ransomware or Trojans undetected.

In cyber attacks which leverage the victim's own programmes, the initial compromise may be executed in many different ways, for instance, the actor may use known methods such as phishing-mails, supply-chain attacks or vulnerabilities in programmes.



Step	How PowerShell can be leveraged in a cyber attack
Reconnaisance	Identifies email-adresses and possible back ground information of victims
Weaponization	Prepares phishing emails with links to malicious homepage
Delivery & Exploitation	1 The hacker sends phishing emails to the victims 2 If a victim clicks on the link, a legitimate programme is started on victim's PC 3 A known vulnerability is exploited in the victim's programme that starts Command Prompt 4 Command prompt starts Powershell
Installation	PowerShell downloads malicious script from the actors server and exectutes it on the victim's system
Command & Control	The hacker sets up infrastructure for communication with the victim's PC
Actions on objectives	The Hacker now has control over the victim's PC and can for example exfiltrate data or download additional malware

Figure 1: Illustration on how PowerShell can be leveraged in a cyber attack

Cyber attacks that leverage the victim’s system require a more active defense

A more pro-active and holistic approach to network defence is needed to detect and mitigate attacks that enable hackers to leverage victim’s own programmes. Consequently, organizations need to implement precautionary measures that prevent hackers from abusing their systems, but it is also vital to have the resources to detect such a compromise.

Some countermeasures require a lot of resources, but one relatively simple way to mitigate this attack technique can be to limit the use of some programmes to relevant users only, in the organization. Many users in public authorities typically have no use of IT administration programmes, and by removing their access to these programmes, the organization may reduce the attack surface.

When hackers still succeed in abusing legitimate programmes, it often requires more protection than traditional anti-virus solutions may offer. This is due to the fact that traditional antivirus solutions typically identify malicious activity in a network or on a unit based on file analysis, or in some cases, processes. Thus, an antivirus solution analyses whether files on the unit or network are malicious based on signatures. The antivirus can subsequently erase files or quarantine them based on the signature in case of a malware.

Attacks that leverage the victim’s own programmes can be challenging because the programmes are legitimate and usually have permission by the antivirus to execute commands. In addition, the malicious activity can be executed fully or partially fileless as described above.

In order to detect this attack type, it is not adequate to scan downloaded and executed files. Detection of the attack technique requires analysis of the activity of the legitimate programmes usually used by the private company or public authority. This can be achieved with so-called endpoint-based programmes that monitor the individual user’s PC. Intrusion Detection Systems (IDS) can also be used to monitor network traffic and detect parts of the attack technique; for example, when an actor pivots from machines in the network. See additional recommendations on how to mitigate these attacks in the end of this threat assessment.

Attacks that leverage victims’ programmes are more frequent

In recent years, there have been numerous cyber attacks during recent years, where actors have leveraged victims’ own programmes, including against Danish entities.

The technique is used both in advanced cyber attacks and in simple, less targeted attacks by less skilled actors. It is likely that the attack technique will be used more often in the future.

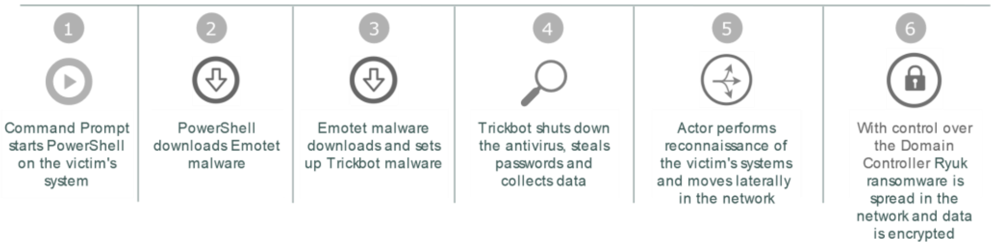

1
Command Prompt starts PowerShell on the victim’s system
2
PowerShell downloads Emotet malware
3
Emotet malware downloads and sets up Trickbot malware
4
Trickbot shuts down the antivirus, steals passwords and collects data
5
Actor performs reconnaissance of the victim’s systems and moves laterally in the network
6
With control over the Domain Controller Ryuk ransomware is spread in the network and data is encrypted

Figure 2: Example of a cyber attack, where the victim’s own programmes is leveraged to spread ransomware on the victim’s network

Cyber attacks where victim's programmes were leveraged

In February 2019, the Norwegian software company Visma announced that it had been compromised. The IT security company that reported on the cyber attack pointed out that the actor had leveraged programmes on Visma's systems in the attack. The report also stated that the actor had previously used the same attack technique against other targets.

According to open sources, the actor behind the LockerGoga malware, which amongst other targeted Norsk Hydro in March 2019, also leveraged the victim's own programmes. The actor leveraged Windows programmes to spread the malware.

Windows software is often leveraged in cyber attacks

Many programmes are being leveraged in cyber attacks by state- sponsored hackers or cyber criminals. These programmes are not leveraged because they are more vulnerable than other programmes, but rather because these programmes are often accessible and relatively simple to use, and also very effective tools in the hands of the hackers. In addition, they hide the hackers' activities, as they are using tools that are pre-installed on the targeted machines.

Hackers often leverage programmes in an attempt to elevate privileges allowing them to create their own administrator accounts with the purpose of pivoting to other machines on the network. This is also referred to as lateral movement in a network.

PowerShell is one of the preferred programmes for hackers to use in cyber attacks, and it is likely that PowerShell will be leveraged more often in cyber attacks in the future. PowerShell has the advantage, that it can be used for fileless attacks which makes detection of malicious activity even harder.

PowerShell may be used for reconnaissance or execution of code directly on the victim's unit. Hackers can leverage the programme to bypass a firewall, shut down an antivirus, install malware or attempt to pivot to other networks in the company or the authority.

Actors often try to cover their activity in the network by obfuscating the malicious PowerShell code executed on the victim's system. Hackers thereby try to avoid, that the code can be read manually. This can for example be encoding in Base64.

Examples of programmes leveraged in cyber attacks

PowerShell: Windows PowerShell has been part of Microsoft Windows for several years. It was developed for system administration such as configuration and task automation.

PowerShell can be leveraged to obtain full control over system functions in Windows. In addition, the actor may leverage PowerShell to run malicious commands directly into the memory of the victim's system.

Windows Management Instrumentation (WMI): Is an administrative tool used for administering servers and units on a network. WMI may be used for configuration of a range of system and security settings.

WMI can be leveraged for several malicious tasks amongst other to perform reconnaissance or lateral movement in a network.

PsExec: Is a tool which can be used remotely to execute processes directly on other units. Commands are sent via Windows Command Prompt.

PsExec can be leveraged for lateral movement in a victim's network.

Pentest-tools also use the attack technique

In recent years PowerShell has been incorporated as a central part of several pentest-tools. This makes it relatively easy for hackers to use the attack technique.

There are various pentest-tools designed for hacking purposes. These tools have been developed by IT specialists for security investigation and for testing IT security in organizations. They can however also be used for malicious purposes. Pentest-tools are publicly available and many are available on the Internet free of charge.

Incorporation of PowerShell in Pentest-tools has made it very easy to leverage the programme in cyber attacks.

Pentest

A penetration test is an exercise where a team of ethical hackers conduct cyber attacks against selected systems to test and evaluate the cyber security. A pentest can thereby help to set the grounds for a risk assessment of an organisation's IT security.

Popular open-source tools that can leverage PowerShell

Cobalt Strike

Software developed to simulate advanced cyber attacks for legitimate security investigations. It is made up by several modules with different attributes for executing a cyber attack ranging from reconnaissance to phishing and post-exploits tools and more. Post-exploit Cobalt Strike maybe used to execute commands, key-logging, transfer of files, escalation of privileges and lateral movement in networks.

PowerShell Empire

Designed for security investigations as a tool to simulate state-sponsored cyber attacks. The tools makes it possible to perform lateral movements in networks, hereby escalation of privileges, key-logging and to exfiltrate passwords or information.
PowerShell Empire is primarily used post-exploit and is based on PowerShell. However, it also has other modules, which may be used for launching cyber attacks with malicious DLL files.

Mimikatz

A tool designed to steal passwords and escalate privileges in various ways, for example by pass-the-hash. Mimikatz' many functions can be automated with PowerShell, thus allowing hackers to quickly move around a target's network.
Mimikatz is often found as a module in other Pentest-tools, for example Cobalt Strike and PowerShell Empire.

There are many other effective Pentest-tools than those listed above, for example Kerberoast.

Pentest-tools are also frequently adjusted. Some developers of pentest-tools have begun writing in .NET C# instead of, for example PowerShell. This was changed in the pentest-tool BloodHoundAD, likely due to the fact that some companies have begun to limit the access to PowerShell in their networks.

It is prolific for hackers to use pentest-tools as they can use programmes, which are already available on the targeted network, for example PowerShell, to expand their understanding and access to a network often without having to use advanced malware to achieve their end goal or actions on objects. This corresponds to step seven in Lockheed Martin's Cyber Kill Chain®-model. Both state-sponsored actors and cyber criminals use these tools in cyber attacks.

In February 2019, a Maltese bank, Bank of Valetta was the target of a digital bank robbery. The actor attempted to steal EUR 13 million. It is likely that the actor leveraged PowerShell in the attack.

Pentest-tools are also used by groups and individuals with relatively limited technical skills, as the tools are relatively intuitive and easy to use.

Developers of open-source tools are often swift to support their tools with the newest vulnerabilities shortly after a vulnerability has been made public or used in the wild by hackers. For example, the BlueKeep vulnerability, which was made public by Microsoft in mid-May 2019, was incorporated in a pentest-tool in July 2019.

Advisory

Despite the nature of the described cyber attacks an organization may still limit the risk of being compromised. The primary focus should be to deter potential attacks from the organization's networks and systems. This is best achieved by, for example, following the recommendations in CFCS's guideline "Cyberforsvar der virker". This will deter a great deal of cyber attacks.

Even if you follow the best advisory, it is unlikely that you will be able to deter all attacks. Therefore, an organization will benefit from implementing a further range of security measures. Even though many of them can be circumvented, it is still relevant to consider implementing them, as they can delay an attacker and thereby increase the chance of exposing the cyber attack.

Organizations should continuously consider the need of having tools installed which are not being used. The advisory below is focused on PowerShell, as the threat assessment has this tool in focus too. Much of the conditions in the advisory below does however also apply to other tools than PowerShell.

Make assessments of the organization's need for PowerShell on the individual PCs or servers. If not, PowerShell should be uninstalled. If there is, make sure to limit the access to and functionality off PowerShell. The functionality may, for example, be limited by use of "Constrained Language mode", which is available in PowerShell from version 5. By this, you limit the possibility to run malicious scripts such as Invoke-Mimikatz. It is recommended, that you always use the latest version of PowerShell and uninstall previous versions.

In relation to protecting passwords in the system there is a function in Windows Defender, Windows Defender Credential Guard, which can make it harder for attackers to steal and exploit passwords. More information on how the function can be used can be found on Microsoft's homepage under the subject: "Manage Windows Defender Credential Guard".

In the guideline "Cyberforsvar der virker", which is only available in Danish, one of the basic security measures is whitelisting of programmes. For this AppLocker can be used, which is included in Windows 10. AppLocker can be used to limit which PowerShell-scripts, that can be run. Be aware, though, that due to limitations in AppLocker this form of protection can, unfortunately, be circumvented.

It is possible to activate and collect a range of logs in PowerShell version 5 hereby potentially revealing unwanted or malicious activity. Logging should be conducted on different levels, in order to increase the change of revealing unwanted or malicious activity. Organizations should activate:

- Script block tracing, that collects all blocks of PowerShell scripts which are run.
- Module/Pipeline logging, that registers all details about what PowerShell is running including which coding modules that are included.
- Transcription, that will create a post in the log for each PowerShell session and include all input and output that occur in this relation.
- Engine Lifecycle logging, that logs start- and termination of PowerShell hosts and all parameters (values) which is send or received from the host. Engine Lifecycle logging is activated by default.

Generally, all logging and collection of these from equipment and systems of an organization's infrastructure is crucial in order for public authorities and private companies' abilities to detect a cyber attack quickly and effectively cover its consequences. For more information about logging please see CFCS's guidance "Logning – en del af et godt cyberforsvar", which can be found in Danish on CFCS's homepage.

For more information on PowerShell setup please see the Australian Cyber Security Centre's guidance "Securing PowerShell in the Enterprise", which is continuously updated.

Besides this it is recommended to read the Australian Cyber Security Centre's guideline "Essential Eight", which lists a range of short and concrete recommendations on how to generally reduce the attack surface for hackers.

Segmentation of the network

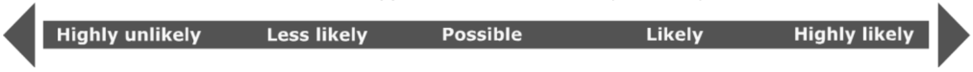
Another measure may be to look at the topology of your network and if possible to split this into a range of segments (security zones). Segmentation of a network provides a lot of security for relative few resources. The purpose of segmentation is to create two or more independent environments, such that an attacker, virus or malware do not have access to the whole network at the same time. Besides this segmentation gives the opportunity to implement different kinds of security procedures and technical measurements in different segments on the basis of the individual segment's criticality.

The CFCS recommends these four steps when segmenting the network:

1. Identify groups of components or networks, that have needs to communicate in relation to business.
2. Assess if there are needs for further security zones in relation to the business communities on the basis of the different security needs.
3. Define which connections between the security zones that are necessary in order to accommodate the business.
4. Establish and maintain an overview, such that there is only one connection or point of information sharing between different segments or security zones.

After having chosen the proper segmentation you can proceed with assessing how the connections are best protected, including the choice of technical measures, setup of jump-stations, de-militarized zones, logging- and detections mechanisms. Backup and system recovery should have special considerations in connection to segmentation. As a starting point backup should be stored in a separate network.

The DDIS applies the below scale of probability


Highly unlikely
Less likely
Possible
Likely
Highly likely