|  |  |  |
| --- | --- | --- |
| Methods of Data Exfiltration | Pros For Attacker’s Use | Cons For Attacker’s use |
| Automated Exfiltration | -Exfiltration Size can be extraordinarily large due to the packet capturing substantial amounts of data coming in extremely quickly and transferred to an unknown location not set. (autoScript)  -Automated exfiltration is easily accomplished in our own environment due to ready-made tools for attackers and with the reliance of powershell.exe commands to simplify the entire process. (autoEase) | -Easy Mitigation due to being based on the abuse of system features only. (auto)  -Easy detectability due to the large amount of data transfer limits and available query scripts available to the open public for detection and mitigation. (autoScript)  -Unrecognized scripts and process file access makes this exfiltration easier to detect as well. (auto) |
| Traffic Duplication | -harder for detection due to looking into packet contents for communications that do not follow regular behaviour, as well as unusual network communications that have never been seen before -require someone more knowledgeable in what is common in traffic flow-. (dupli)  -easily accomplished using commonly accessed and open-sourced tools meant for automatically cloning traffic packets. (clone)  -Exfiltration size can be large due to the consistent cloning of the original traffic towards the attacker’s PC for analysis. (dupli) | -Easy Mitigation due to just the requirement of encryption for sensitive information as well as authentication. (dupli) |
| Data Transfer Size Limits | -easier avoidance to data transfer alerts (size)  -harder to mitigate due to the requirement of Network Intrusion Prevention systems for looking into the signatures and the ease of which to hide them. (size)  -easily accomplished with open-source tools that are widely distributed, such as cobalt strike or RDAT. (size)  -size limit is fixed however this means that it can go through and bypass certain queries due to not breaching the limit. (size) | -Easy to detect due to the need to just look into the creation of additional network connections and flow in which if there is a suspicious consistent amount of data flow. (size) |
| Exfiltration Over Alternative Protocol | -size limit is dependent on the protocol used; this means that attackers can make their attack seem more natural with more normal looking size of output in terms of the network protocol used in order to hide against initial scans. (alternative)  -due to the wide arrange of protocols that could be used to carry information, attackers have a wide array of choices to accomplish this method of exfiltration to suite their specified needs. (alternative) | -easier mitigations due to the wide array of controls available such as blocking sensitive data, filter for only allowing authenticated servers to communicate, looking into signatures for this exfiltration, and the use and configuration of firewalls that are readily available. (alternative)  -easy for defenders to detect this due to the strict use of command prompts, looking into the file access for validation, and the contents of the network traffic. (alternative) |
| Exfiltration Over Symmetric Encrypted Non-C2 Protocol | -more complex mitigation efforts must be established to thwart this method due to the complexity; this includes the skillset required to segment the network and effectively use firewalls and filter and detect any command signatures used in accomplishing this act. (symmetric)  -exfiltration size is smaller which allows for the exfiltration over a symmetrically encrypted network and send to the desired server/location. (symmetric) | -due to the use of easily readable commands and data being used, this method is extremely easy to detect as the defenders can just look at the commands used, file accessed and the content of the network connections themselves. (symmetric)  -due to the dependency on certain network designs this method is not easy to setup and use as each network is encrypted differently depending on the wide array of algorithms in place. This would also mean that attackers using this method would have to go through multiple layers of encryption which would be challenging to accomplish. (symmetric) |
| Exfiltration Over Asymmetric Encrypted Non-C2 Protocol | -the size of the exfiltration can very depend on the encryption algorithm; this means that attackers can hide the transfer of sensitive data over a network towards their destination with ease. (asymmetric) | -easy mitigation due to the use of data loss prevention systems which track and block the data going through the network, as well as the filter of traffic itself and segmentation, and prevention with this method having a clear signature to track, as well as the fact that it moves easily detectable data across. (asymmetric)  -simple detection due to the use of looking into the file access, commands executed, and the network traffic contents themselves. (asymmetric)  -hard to setup due to the requirement of obtaining a key from the victim itself, making this setup and usability more complex. (asymmetric) |
| Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol | -harder to detect due to the requirement for analysis of the behaviour of certain servers. (unencrypt)  -easy to accomplish due to the unencrypted protocols being simpler to manage such as the transfer of sensitive data over FTP. (unencrypt)  -exfiltration size can be large due to the unencrypted channels having less headers and thus more room to move the large amounts of sensitive data. (unencrypt) | -more simple mitigations due to the use of preestablished data loss prevention systems which block the data over the unencrypted protocols, which can be contained through further network segmentation and filters. (unencrypt) |
| Exfiltration Over C2 Channel | -harder to detect and mitigate due to the use of preestablished command infrastructure and resources, as well as the use of encoding to hide it through normal communications. (c2)  -easier to accomplish and setup due to the use of the resources available in the client as well as the abundance of automated scripts to allow for this accomplishment. (c2) | -size is dynamic as it must mirror the environments average communication size which depends on the environments use itself. This can make it harder to determine the appropriate size. (c2) |
| Exfiltration Over Other Network Medium | -size of exfiltrated data may be phenomenally huge to the repeated transfer of smaller data sections through use defined events which may occur multiple times or just once which would allow it to stay hidden under automated network defenses. (network) | -Hard to setup and use due to the requirement of sufficient access/proximity to the area as well as the fact that the connection must already be not secure or encrypted. (network)  -easy to mitigate due to the simplification of configurating the OS to block the creation of new network adapters where applicable. (network)  -easy to detect due to the use of monitoring just for changes to the host adapter settings, and user driven events that may lead to malicious code. (network) |
| Exfiltration Over Bluetooth | -easier to setup due to the requirement of unsecure Bluetooth devices in which consumers may easily overlook in terms of security. (bluetooth)  -size of the exfiltrated data may vary depending on what the bluetooth device is connected to; this means that attackers may have access to the neighboring machines connected to the device which can later be scaled upwards to the rest of the home network. (Bluetooth) | -Easy to mitigate due to just the simple disabling of Bluetooth related capabilities when not in use. (bluetooth)  -easy to detect as it just requires the monitor for user-driven events as well as changes to the host adapter setting. (bluetooth) |
| Exfiltration Over Physical Medium | -size of data can very to large depending on the removable device itself; this would allow the method or the device to function as the final destination for the attacker to gain access to the sensitive data. (physical) | -hard to setup and accomplish due to the requirement of physical access to the victims pc. (physical)  -easy to mitigate due to the requirement of limiting hardware installation as well as disabling or removing excess features. (physical)  -easier to detect due to just monitoring the local processes occurring when a removable media is inserted and ensuring that the file access is configured properly, and that data has not been accessed by these media drives. (physical) |
| Exfiltration over USB | -due to the available access to usb ports around any infrastructure containing data and the requirement of just automatically copying the files across, this method is easy to accomplish. (usb) | -easy to mitigate due to just simply blocking the transfer of sensitive data across usb devices as well as limiting the hardware to prevent certain access across physical ports. (usb)  -easy to detect as the defender can just monitor for any file access on removable media that was just installed as well as processes that were executed when that, so device was plugged in. (usb)  -size of the exfiltration method is limited to the device itself. This means that the attacker may miss certain precious data when copying the files over and even so may just be stuck with copying only a small portion of it. (usb) |
| Exfiltration Over Web Service | -harder to detect due to the readymade web services providing ample protection with the encryption of stolen data and cover. (web)  -easier to setup due to the existence of legitimate web services to just simply move data across. (web)  -size of exfiltration data is large due to the use of web services providing a reliable connection for the transfer of information. (web) | -easy mitigation due to just the simple restriction of web services. (web) |
| Exfiltration to Code Repository | -easier to setup due to the accessibility of code repositories through APIs and accomplished over HTTPs which allows for more simplified and secure setup. (repo)  -harder to detect due to repositories providing ample cover for the transfer of data. (repo)  -size of the exfiltrated data can very as to mirror the normal contents of the repository server and disguise as a normal outlook of information. (repo) | -simple mitigation due to the restriction of web-based content that could be accessed as well as unauthorized services to be blocked. (repo) |
| Exfiltration to Cloud Storage | -ease of setup is simple as readymade scripts are available to download and modify to copy over the victim’s information towards a cloud storage network. (cloud)  -hard to detect; due to the large amount of use in terms of cloud storage it is easy to hide data exfiltrated over towards the remote storage to act like normal and to bypass network monitoring systems. (cloud)  -size of exfiltrated data can be phenomenally huge as it does not require the purchase of expensive storage equipment as the storage could easily be rented out temporarily allowing for better cover. (cloud) | -easy to mitigate due to just simply blocking the use of unauthorized cloud storage services to prevent data being sent towards a remote location. (cloud) |
| Scheduled Transfer | -harder detection due to the scheduling of data transfers to make the system more hidden to normal monitoring processes while also mimicking regular maintenance. (transfer)  -easier to setup due to the requirement of just having to set up the timer and amount of data to transfer as to blend in with the patterns. This transfer is also automated using open-source tools such as Cobalt strike as well. (transfer) | -easier to mitigate due to looking through the signatures to find indicators of a scheduled transfer while also looking for command signatures as well. (transfer)  -size of exfiltrated is small and overtime due to the need to keep this process hidden. This means that it would take time to gain any meaningful data overall from the organization. (transfer) |
| Transfer Data to Cloud Account | -size of exfiltration data may be limitless due to having full access to companies’ data depending on the role and the cloud storage can be easily scaled up to compensate for the abundance of sensitive information on the organization. (account) | -easy to mitigate due to just limiting user account privileges as well as password policies. (account)  -easy detection due to signatures being the attempts to share data, snapshots of the storage/accounts while also looking into the managed cloud storages for any creation or modifications that usually rarely occurs. (account)  -hard to setup due to the requirement of having the required password and authentication to move the cloud data over to a new cloud storage to then analyze for personal gain. This means that the attacker would be under high surveillance already as an employee while also being managed by the employers in terms of what can be accessed. (account) |

Use Cases and Advantages

|  |  |  |
| --- | --- | --- |
| Methods of Data Exfiltration | Use Cases | Advantages Over Other Methods |
| Automated Exfiltration | Attacker wants to update the data stolen by the corporation dynamically -obtain the latest data or all the data generated currently-, so they automate the process of exfiltrating the data using automated exfiltration to accomplish this. | Less user intervention due to the data exfiltration being carried out automatically. |
| Traffic Duplication | The attacker wants to read into what is happening in the network without raising any suspicion to obtain any data being sent through. This means that the attacker would use traffic duplication to get the same traffic being sent around the organization. | More control/knowledge in what is going on in the organization as well as the ability to obtain highly sensitive data being sent to and from clients. |
| Data Transfer Size Limits | The attacker wants to send the data back to their own server but is scared that the automated defenses would catch on. This means that the attacker would use this method to limit the size of the data to below the threshold in order to hide suspicion. | Increased chance of bypassing automated network scanners that organizations rely on and to make data seem more natural. |
| Exfiltration Over Alternative Protocol | The attacker wants to transfer data over to their own remote storage area however they know that the protocol is actively being monitored for any data going through. They decide to use this method to invade defenders as they would not be paying as much attention to the different protocol for any transfer of sensitive data as it is usually not responsible for this goal. | Increased chance of hiding the fact that data exfiltration is occurring due to defenders not suspecting the protocol being used to transfer data. |
| Exfiltration Over Symmetric Encrypted Non-C2 Protocol | to hide what data is stolen through the network as the network may be monitored for any company data that is sensitive. | Data that is being exfiltrated across the network is unknown to the victim, increases the chance of it being put aside. |
| Exfiltration Over Asymmetric Encrypted Non-C2 Protocol | To hide what data is stolen however using a different encryption channel in order to go through areas that may be of less concern. This also moves the data to a different less defended network area in order to get to the attacker’s storage. | Data exfiltrated are encrypted in a separate channel which makes it even harder for defenders to catch on in comparison to other methods. |
| Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol | To obfuscate the data contents instead as if the data was encrypted then it may draw in more attention to defenders instead of it just being hidden. | Data that is being exfiltrated using this method have an extraordinarily high chance of it being viewed as a natural process or a less important/obscure action that is being taken place, due to the data contents being hidden in comparison to other methods. |
| Exfiltration Over C2 Channel | To steal data using openly available network connections in order to cover their tracks more efficiently. | More easily accomplished due to using preestablished connections that allow the data exfiltration process occurring to become less suspicious. |
| Exfiltration Over Other Network Medium | To use a new separate unmonitored network connection to move stolen data across as these connections are not previously established by the organization so defenders wouldn’t be looking into these network connections. | Increased chance of bypassing network monitors.  To exfiltrate over unmonitored/unrecognized traffic that defenders/victims may not realize yet or thought to monitor in time in comparison to other methods. |
| Exfiltration Over Bluetooth | To obtain data through a less secure and unmonitored/unaccounted for connection that is easily obtainable once the attacker is in the proximity. | Easily obtain data over unsuspecting victims through almost completely unsecure network channels with bluetooth devices. |
| Exfiltration Over Physical Medium | The attacker has physical access to the resources and wants to move the files over quickly with a removable storage due to the network being monitored too heavily. | Easily copy files over directly to the storage device without going through the network monitoring applications. |
| Exfiltration over USB | To bypass air gapped more secure systems in order to steal the data or to copy over data using a more concealable object as normal physical medium may catch unwanted attention. | Ability to bypass air-gapped systems to exfiltrate extraordinarily sensitive data while also being more concealable. |
| Exfiltration Over Web Service | To steal data more effectively as using preestablished web services to transfer stolen data across is easier than establishing new ones; as it would make the exfiltration of the data harder to detect due to the system moving data already having been authorized for it. | Extremely convenient to setup and provide ample cover for the data exfiltration process from monitoring systems. |
| Exfiltration to Code Repository | To provide more cover for the exfiltration of data to have a higher chance of success, as the attacker wants something more easily available to move the data to. | Openly available storage areas for the exfiltrated data while providing an abundance in secure encryption to hide from prying network monitors. |
| Exfiltration to Cloud Storage | To have more control of the data that is being exfiltrated as well as to have more scalable space if the data being exfiltrated is large-scale. This is also to provide more added cover due to cloud storage providers being commonly used to move data over. | Easily accessible and reliable storage space for the data exfiltration to occur for while providing an abundance of cover due to the activities of the storage system matching the data exfiltration process. -normal process and malicious both transferring authentic and sensitive data- |
| Scheduled Transfer | To bypass automated active network monitoring tools and to make the data being exfiltrated seem like a normal process more. | Extremely hidden towards automated scripts and monitors due to the data exfiltration being more natural looking and least suspicious out of all of them. |
| Transfer Data to Cloud Account | To change the cloud account in where the data is normally saved, to allow for more harder to detect and almost unnoticeable data exfiltration as the cloud service was already commonly used while also still allowing the capture of large-scale sensitive information from the organizations. | Streamlined data exfiltration process in terms of using the same web service while making the data exfiltration process more unnoticeable to the naked eye as this process mimics the natural activities of backing up and storing sensitive data, while in reality it is exfiltrating the data out to an unauthorized attacker. |

References:

[auto] <https://attack.mitre.org/techniques/T1020/>

[autoScript]<https://community.sophos.com/intercept-x-endpoint/i/att-ck/mitre-att-ck-exfiltration-tactic>

[autoEase]<https://github.com/benstew/awesome-data-exfiltration#-physical-mediums>

[dupli]<https://attack.mitre.org/techniques/T1020/001/>

[clone]<https://research.nccgroup.com/2021/05/27/detecting-rclone-an-effective-tool-for-exfiltration/>

[size]<https://attack.mitre.org/techniques/T1030/>

[alternative]<https://attack.mitre.org/techniques/T1048/>

[symmetric]<https://attack.mitre.org/techniques/T1048/001/>

[asymmetric]<https://attack.mitre.org/techniques/T1048/002/>

[unencrypt]<https://attack.mitre.org/techniques/T1048/003/>

[c2]<https://attack.mitre.org/techniques/T1041/>

[network]<https://attack.mitre.org/techniques/T1011/>

[bluetooth]<https://attack.mitre.org/techniques/T1011/001/>

[physical]<https://attack.mitre.org/techniques/T1052/>

[usb]<https://attack.mitre.org/techniques/T1052/001/>

[web]<https://attack.mitre.org/techniques/T1567/>

[repo]<https://attack.mitre.org/techniques/T1567/001/>

[cloud]<https://attack.mitre.org/techniques/T1567/002/>

[transfer]<https://attack.mitre.org/techniques/T1029/>

[account]<https://attack.mitre.org/techniques/T1537/>