HISCOX

CYBERCLEAR®

Data exfiltration during ransomware attacks

Data exfiltration by hackers is not new. Neither is ransomware. According to the Hiscox Cyber Readiness Report 2020, 16% of the 5,569 companies surveyed paid a ransom; 19% of the sample had experienced ransomware but restored data through back-ups. The use of both exfiltration and ransomware together in a combined attack has also been seen before. But it certainly seems that cybercriminals are starting to use this combination with increasing success.

In the last six months, high-profile ransomware cases such as Toll Group and Allied Universal have brought to light the effectiveness of this combination. Hackers are using the threat of publicly leaking and auctioning stolen data as further leverage to persuade victims to pay the ransom or face embarrassment and brand damage. It's a difficult position for anyone to be put in.

But large-scale data exfiltration is a tricky business to be in if you are a hacker. It is a very different style of attack compared to ransomware, and it requires different skills and tools to be successful. Hackers know this. The recent cases we have seen using data exfiltration as a means to further encourage the victim to pay the ransom have not involved particularly large volumes of data – in fact the attack against Allied Universal only involved the exfiltration of 5GB of data, which is small by modern standards.

What we see here is hackers being selective about the data they are stealing, aiming for low-volume high-impact data, versus stealing any significant volume. Allied Universal, as an example, had sensitive business files and cryptographic keys stolen – not reams of personal data.

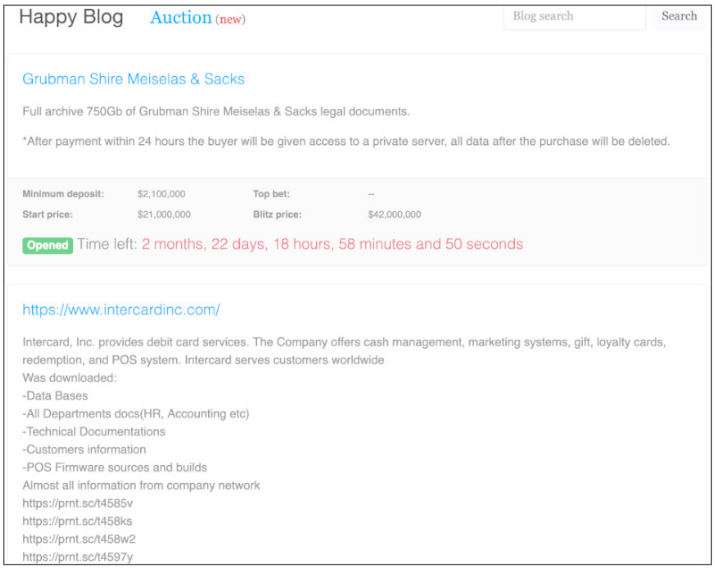
How is data exfiltration done?

With the ever increasing interconnected nature of our organisational networks, and the proliferation and use of internet-based cloud services, unauthorised data exfiltration can now be done in many different ways.

This can be as simple as access to a compromised corporate email account to send and receive files outside of the network. The credentials for this could have been harvested during the initial ransomware attack. Or it could involve hackers building-out their own infrastructure on the internet for larger-scale operations.

This is a technique sometimes referred to as 'hiding in background noise' or in dedicated data exfiltration campaigns this is known as a watering hole technique. Taking data little and often is less likely to be blocked than a single large transmission. As such, the value of the data stolen is maintained. If lots of credit card data is stolen and reported, these card details will be worthless to a hacker.

If they are not reported as stolen, they can be worth a great deal and sold on the DarkWeb (see image).



No matter how advanced our security arrangements, it can be very difficult to isolate illegitimate from legitimate communications on a network when there is no obvious change in the network behaviour. And hackers generally know this. Large scale smash-and-grab style data exfiltration is often noisier and easy to detect, which is probably why we are seeing ransomware attacks use a more discreet approach to data exfiltration.

Hiding in background noise

A watering hole technique. Taking data little and often which is less likely to be blocked than a single large transmission.

Some common data exfiltration techniques

Good old-fashioned email

Some families of malware are dedicated to data exfiltration and include the tools necessary to remove data from a network. This can include the use of trojans, such as Emotet, which provide a covert channel in and out of the target organisation. These are commonly used by hackers to gain entry to a network so that they can download more of their software on our network, or in reverse to transmit data being exfiltrated.

Some mail-filtering technologies can also be overcome by using a dead letter box – that is simply creating a draft copy of an email with attachments and accessing the files from the draft folder before filtering technologies can kick-in. No matter what, it is always a good idea to block compressed and encrypted files from entering and leaving your network via email if you cannot inspect them first. Of course this will frustrate some business users, so offering an exception process for legitimate business use might be necessary.

Instant messaging and team collaboration services

Modern instant messaging services such as Skype, and collaboration tools such as Slack and Trello, offer organisations the opportunity to work with remote teams from their own businesses and with third parties. Many of which of are typically internet enabled cloud services. Most of these modern tools also offer file sharing services which offer hackers another route for shipping data outside of your business, which may not be being monitored.

Most of these services only offer small file upload sizes, usually on average 1GB per message up to a maximum of 10GB of storage per user. This limits the volume of data that can exfiltrated at any one time, although low-volume high-value data is a good candidate for this method. This is why some businesses restrict instant messaging services beyond their own corporate users.

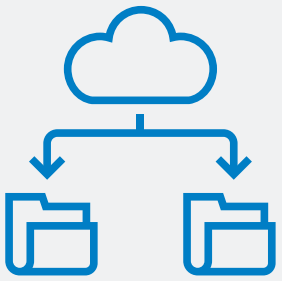
File sharing services

To exfiltrate larger volumes of data out of a network, email is not ideal. It can often be readily detected and blocked. This is when file sharing sites and services come in handy if you're a hacker. Services such as Dropbox, Google G-suite and Microsoft OneDrive all offer the ability to upload large volumes of data and share them with people outside of your own organisation – often for legitimate business reasons. Sites like Pastebin, Github and YouTube can also be used. All of these services offer hackers a simple route to move data outside of our business.

Many businesses choose to block these types of internet service for exactly this reason. And this is typically good advice. If there is no legitimate need for users to utilise a Dropbox-type service, then restricting access to these services will help minimise data exfiltration routes from your network and generally make life harder for hackers. This course-grain approach, however, comes with a difficult balancing act and may involve blocking services commonly used for genuine business reasons. This is where content inspection technologies can come in very useful to give you a fine grain level of control over the types of data being transmitted.

Large scale data exfiltration

If you are running file transfer protocol (FTP) network file share (NFS) or server message block (SMB) these offer hackers a route for larger scale data exfiltration.



Malware

Some families of malware are dedicated to data exfiltration and include the tools necessary to remove data from a network. This can include the use of trojans, such as Emotet, which provide a covert channel in and out of the target organisation. These are commonly used by hackers to gain entry to a network so that they can download more of their software on our network, or in reverse to transmit data being exfiltrated.

Misuse of network sharing protocols

Hackers will often look to exploit the victim's own technology where ever possible. So if you are running protocols on the network that already offer the ability to export data to a remote destination on the internet, such as file transfer protocol (FTP) network file share (NFS) or server message block (SMB); then these offer hackers a route for larger scale data exfiltration. They can also offer hackers the opportunity to import their own malicious software to your network. As such, many organisations choose to severely limit or prohibit the use of these protocols across internet boundaries.

More advanced techniques such as data pumps

Where large-scale data exfiltration is the name of the game, hackers will often need to build out their own infrastructure on the internet. This could be as simple as their own file transfer website, through to more sophisticated techniques, such as data pumps. A data pump allows a hacker to export entire databases using the inbuilt functionality of a database to export data to another remote database location. Data pumps can be configured on a timed basis to ship data when the network is quietest, or to throttle the transmission of data to prevent network performance issues being reported by legitimate users. All of these can be used to help the data export go undetected.

What can we do to help prevent data exfiltration?

Block file sharing services where ever possible

If you don't need to use third-party file sharing sites such as Dropbox, be sure they are blocked on your network. This type of site provides an easy way to exfiltrate moderate volumes of data from a network with great ease. Dropbox as an example allows for up to 50GB of data to be transferred at a time. All that is needed is an internet connection.

Enable email filtering

Inspect all email entering and leaving your organisation. This can be achieved in many ways including the creation of simple outbound mail content rules on your Exchange server through to third-party mail filtering services such as Mimecast. Ensure content inspection is enabled and decide what to do with email that cannot be inspected – such as encrypted or password-protected attachments. In general, if you cannot inspect it then don't let it leave your organisation.

Regularly patch all your technology

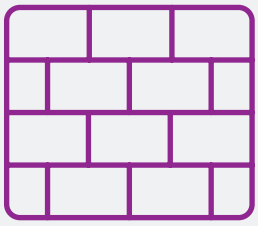
Hacking usually involves some exploitation of a technical vulnerability, so make sure that IT systems are patched as frequently as practical. This needs to include operating systems, all software applications including browsers, databases, network appliances and protocols. Make sure you know exactly what software is installed on devices and leave nothing unpatched for any prolonged period of time. Sign-up for automated vendor notifications on patches so you can keep a track of any new releases as soon as they become available.

Use a reputable anti-virus product

Modern anti-virus technologies are often able to analyse operating system behaviours, such as CPU utilisation and file permission changes, ensuring that any unusual activity on a device doesn't go unnoticed. Ensure that the anti-virus software is routinely updated as these vendors frequently release updates in response to the latest threats. Many operating systems vendors, including Microsoft and Apple, now incorporate anti-virus technologies in their products by default.

Next generation firewalls

Companies including Fortinet and Barracuda allow for network traffic to be inspected with a greater degree of granularity than more conventional firewalls.



Use an internet proxy

Route all of your internet traffic via a proxy, regardless of if it originates on or off your domain. Remember that mobile or remote users may not be connected to your corporate network all the time, and ensure that device configurations are set to send all internet connections via your proxy service. This is relatively easy to establish and ensures that all internet traffic goes via one route which means you can inspect and control it.

Inspect network traffic where possible to look for unauthorised data transfers

Next generation firewalls, such as Fortinet and Barracuda, allow for network traffic to be inspected with a greater degree of granularity than more conventional firewalls. Ensure that rules exist for compressed file formats and encrypted content inspection. If you can't inspect the data leaving, then consider blocking it by default and triggering an alert to systems administrators or security teams. Getting this control right does involve some technical tricky and may require some specialist security guidance.

Identify and block unauthorised configuration changes

Hackers routinely change the configuration settings of technology to allow them greater access and mobility across networks. This could involve changing firewall and network routing rules, disabling security software (such as the use of anti-virus) or disabling the creation of security event data. Good configuration control and change management processes will help ensure that only authorised changes can be made to system configurations and help detect attempts to change configurations without approval. This should also include attempts to introduce any new software to a device or server that does not form part of its baseline configuration.

Hunt down your dormant, orphaned or duplicate accounts and remove them

People come and go from organisations all the time – whether permanent staff, contractors or consultants. Sometimes they leave behind a legacy of credentials they were using to access our networks and systems. Dormant accounts are those that are no longer required. This could be temporarily dormant due to maternity leave, or permanently dormant due leaving our organisation. Orphaned accounts are typically application level accounts, or those not bound to our main network identity, which get left behind when the primary login account is deleted. Duplicate accounts are those where a single user has multiple accounts for our systems or networks.

All of these offer hackers an opportunity to gain access to an account that no-one else is currently using, which means they are less likely to get spotted using it than with an account that another user routinely accesses. No matter how good we believe our joiner/mover/leaver process to be, we should routinely hunt down these accounts, check for any signs of unauthorised use and then remove them.

Apply good access controls to data

Not everybody in your organisation needs access to all of your data. This is sometimes referred to as the 'need-to-know' principle. Whilst generally good practice in any business, minimising accessing to your data to the fewest people possible makes it much harder for a hacker to access a wide spectrum of data for exfiltration from a single account. If they have compromised a user account, they will initially be limited by the level of access that account has. This is why administrator credentials are favoured for compromise as these typically have greater degrees of access to your systems. Be sure to safeguard these accounts carefully, and spread administrator permissions across several accounts or minimise their individual access where ever possible. Try to routinely review user access to data, sometimes known as authorisation management, to remove any unnecessary permissions.

Security monitoring

In our opinion, security monitoring is the most essential ingredient for protecting an organisation against any form of cyber attack – including ransomware and data exfiltration. If we can't see it is happening then we can't do anything about it.

No matter how robust our security is, or how 'unhackable' we might believe we are, all security controls will eventually fail if left unchecked. This category of control often requires investment and ongoing development to be meaningful. It helps us build an understanding of what normal means on our network which helps us identify anything abnormal so that we can respond accordingly. The most mature security arrangements in any organisation will typically be centred around this type of capability.

Gathering event data from a multitude of different sources, such as operating systems, applications, databases and firewalls provides a holistic picture of what is going on in the network. Using centralised event stores allows for the analysis of this data to take place in a meaningful time frame. Adopting security monitoring tools such as Splunk or QRadar allow for automated alerting of suspicious activity, and even machine learning to help identify patterns in the data collected. But someone needs to look at this data and respond, and that's where continuous training and rehearsals become essential for security operations teams.

We recommend paying particular attention to events generated from any privileged user account, such as operating systems administrators, database administrators and network engineers. Signs of large scale data exfiltration might include new network routing rules being created, slower than usual network performance, unusually high CPU utilisation on a device and users complaining about applications and databases running poorly or becoming unusable.

Enable multi-factor authentication on web enabled services such as email

Where internet enable services are used by your organisation, ensure that multi-factor authentication is enabled – preferably using an authentication app on a mobile device. This could include Office365, G-Suite, Slack or any other software as a service applications you are using. This will help prevent them from being used to exfiltrate data from your network.

Pen testing and red team activities

If you want to see yourself safely through the lens of a hacker, then there is great merit in undertaking routine penetration tests or simulated attacks via a Red Team. Not only will this give you invaluable insight to how a hacker may compromise your network (and in turn how you can prevent it), if you have a security operations team monitoring your network it will give them useful experience and provide you with assurance about effectively they can detect and remediate potential problems.

Cyber criminals never stop evolving

The tactics are not new, but the increased use of data exfiltration in combination with ransomware requires a shift in strategy. Assess if you're currently mitigating against data exfiltration and exercise as many preventative measures as possible. Cyber criminals never stop evolving, neither should we.

HISCOX

Hiscox
22 Bishopsgate
London EC2N 4BQ
United Kingdom

T +44 (0)20 7448 6000
E enquiry@hiscox.com
www.hiscoxgroup.com

20816 07/22