Data Exfiltration Techniques (An Incomplete List)

By Ben Stewart

A security vulnerability is a specific weakness. An exploit is an attack that takes advantage of a vulnerability to gain access or some form of control over a network or system. For example, a successful exploit of a SQL injection vulnerability could be used to collect records from a given database. By understanding the difference between what is vulnerable and what is exploitable, can help an organization to prioritize and appropriately assess risk. Then by demonstrating post exploit techniques, we can more appropriately prepare organizations for defending against real-world attacks.

A successful exploit commonly results in some form of a data breach or privilege escalation. Data exfiltration is the unauthorized transfer of data from a target's network to a location that a threat actor controls. The recipient could be a hacker, a disgruntled employee's thumb drive, or anywhere in between. What makes data exfiltration so dangerous is that it can be done manually, via malware, or remotely with automated tools, making it a big internal and external risk.

Like most cybersecurity threats, there is no silver bullet solution. Further complicating the problem, many organizations aren't able to conduct the necessary threat modeling and asset discovery to understand their IT systems -- so how can they protect them? The shift towards the cloud and remote work arrangements increase the potential attack surface. To address data exfiltration risk, organizations tend to beef up perimeter and end-point defenses with technologies such as DLP. However, these can and will continue to be circumvented.

With the right know-how and specialized tooling, an informed security person can tackle this problem effectively. I've put together a list of publicly available data exfiltration tools that can help conduct complex tactics for data exfiltration, but let's first examine attacker techniques to put them into context. The exfiltration techniques mentioned below were heavily influenced by the MITRE ATT&CK Matrix for Enterprise.

Attacker Techniques

Alternative Protocols

Data exfiltration is often performed with a different protocol from the main command and control (C2) protocol or channel (e.g.. FTP, SMTP, HTTP/S, DNS, etc)The data can be sent to an alternate network location from the main C2 server. Always follow best practices for configuring firewalls and restrict services appropriately. Detecting data exfiltration using alternative protocols can be done through analyzing network data for anomalies related to specific protocols or ports.

Automated Exfiltration

An attacker may look to exfiltrate data that they have gathered through scripting or automated processes/frameworks. Automated exfiltration can utilize multiple techniques. Whitelisting tools, utilities, scripts, and software used to transfer data can be a good start to limiting the effectiveness of this technique. Monitoring process file access patterns as well as network activity can help with detection.

Compressed Data

An attacker may compress data that is collected prior to exfiltration. This will minimize the amount of data sent over the network and potentially decrease their chances for detection. Compression usually occurs with a custom program, algorithm, or common library like 7zip or zlib. Adopting some form of process monitoring or monitoring command line arguments for known compression utilities can be an effective step in detecting this form of data exfiltration.

Command and Control Channels

Data exfiltration is performed over the C2 channel using the same protocol as C2 communications. Network intrusion detection and prevention systems can be used to help mitigate this technique at the network level. Detection is aided using network data to spot anomalous flows that may exist (e.g. suspicious network communications that haven't been seen before).

Data Transfer Size Limits

An attacker may exfiltrate data in fixed size chunks instead of whole files or they might limit packet sizes below certain thresholds. The goal being to avoid triggering network data transfer threshold alerts. Detecting this exfiltration technique involves analyzing network data for anomalous behavior like fixed size data packets or long running connections at irregular intervals.

Encrypted Data

An attacker may look to encrypt data, prior to exfiltration, to make the exfiltration less conspicuous or to hide from a defender. Encryption is typically done using a utility, library, or custom algorithm. Common encryption files are RAR and zip. Detecting can happen in many ways. One effective technique has been to analyze the entropy of network traffic to determine if encrypted data is being transmitted on normally unencrypted, internal channels.

Other Network Mediums

An attacker can use another network medium than the C2 channel. If the command and control network is a wired Internet connection, the exfiltration may occur, over a WIFI connection, modem, cellular data connection, Bluetooth, or another radio frequency (RF) channel. In addition to monitoring network communications for process with anomalous behavior, monitoring changes to host adapter settings can flag this potential technique.

Physical Mediums

An attacker can introduce a physical medium or device to exfiltrate data. This could be an external hard drive, cell phone, or other removable storage and processing devices. The physical medium could be used to exfiltrate data from even the most secure environments (e.g. air-gapped networks). Detecting this technique can be done by monitoring file access on removable media and identifying processes that execute when removable media are mounted.

Scheduled Transfers

To remain in stealth mode, an attacker may perform data exfiltration only at certain times of day or at certain intervals to blend traffic patterns with normal activity or availability. To detect this technique, monitor network behavior and file access patterns for suspicious activity.

Steganography

Steganography is the practice of concealing messages or information within other non-secret text or data (aka “hiding in plain sight”) There is a wide range of file types and methods of hiding files/data. Using a tool like StegExpose or StegSecret will help with detection.