Ransomware: The Data Exfiltration and Double Extortion Trends

The Multi-State Information Sharing and Analysis Center's (MS-ISAC) Cyber Threat Intelligence (CTI) team assesses it is highly likely ransomware groups will continue to steal and post victim data throughout 2021, as an added revenue generator and double extortion tactic. By threatening to publicly post confidential data, ransomware groups are placing additional pressure on victims to pay out the ransom for the promise of outright deleting or keeping stolen data confidential. Besides publicly posting data, ransomware groups sell stolen data in cybercriminal forums and dark web marketplaces for additional revenue. Data from Chainalysis shows the total amount paid by ransomware victims increased 311% in 2020, amounting to nearly $350 million worth of cryptocurrency. [1] In one high-profile example, a public university reportedly paid over $1 million in Bitcoin to recover its encrypted files and delete the stolen data. [2]

Throughout 2020, the MS-ISAC CTI team observed ransomware groups increasingly turning to double extortion attempts with stolen data, while maintaining the traditional network encryption and ransom routine. Ransomware groups continue to exfiltrate data during intrusions, mimicking the Maze ransomware group's tactic of publishing stolen victim data, which made headlines in late 2019.

Threat to SLTTs

The recent trend of CTAs using data exfiltration as leverage over SLTT victims is especially impactful to organizations housing sensitive information, such as public healthcare entities and K-12 school districts. These public sector targets remain popular because of their essential services and public sensitivity on protecting children and the ill. Thus, these organizations feel an internal sense of urgency joined with public pressure to resume operations quickly, which cyber threat actors (CTAs) are taking advantage of via higher ransom amounts.

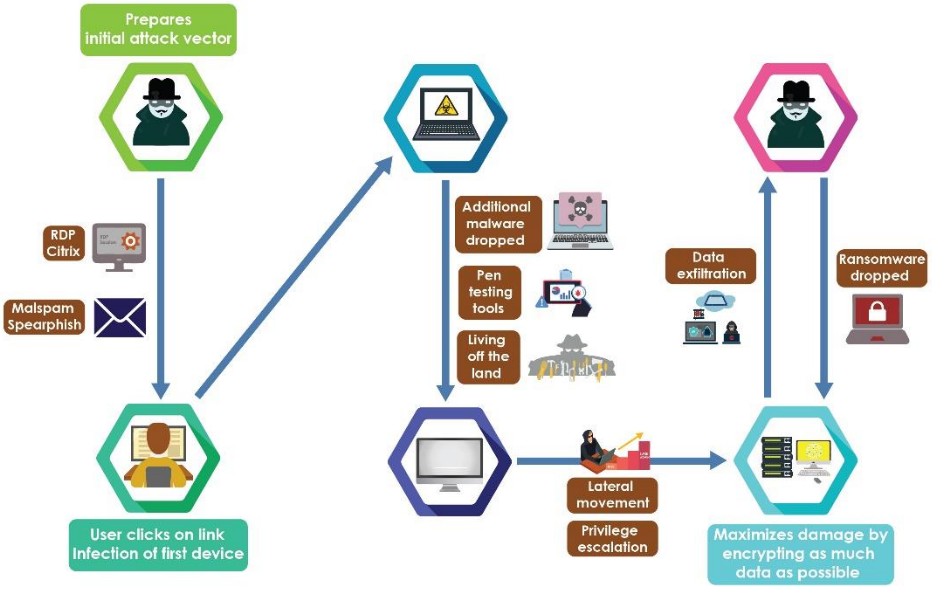
- Healthcare entities are especially vulnerable to data exfiltration as many can only devote limited resources to network security. Phishing is a prominent attack vector used by ransomware groups to gain initial access to a victim's network. Partly due to the fast-paced and critical work environment of most healthcare entities, CTAs are able to maintain phishing operations as a low-risk high reward attack vector. Ransoming the healthcare sector also enables CTAs to leverage critical care services and vital data to pressure healthcare providers to pay the ransom. [3] In September 2020, CTAs breached and exfiltrated data from a university hospital with folders containing "appointments, archives, notice of claims, agreements, litigation files, employment and labor, and credentialing and disciplining (sic) of physicians, among others." [4] Leaked protected health information (PHI) is a serious concern for healthcare organizations that may face litigation as a consequence of improperly securing PHI data in violation of HIPAA.

- K-12 school districts represent another popular SLTT target for ransomware groups. These institutions tend to have limited IT and cybersecurity resources and often a flat network architecture. In 2020, many K-12 school districts were infected with ransomware and often exhibited higher tendencies to simply pay the ransom. The noted lack of network segmentation makes it easier for ransomware groups to move laterally in K-12 networks to quickly harvest large amounts of data, which is then exfiltrated off the network and encrypted on premise. School districts of various sizes were victims of these types of attacks. CTAs were also observed posting data to the dark web, which potentially included grades, financial, medical, and disciplinary information on students.

If an organization is initially unwilling to pay the ransom, CTAs can use data leak sites to post portions of the data, attempting to increase their leverage and potentially shame the victim. CTAs might also sell or auction data if an organization does not pay the ransom. Popularized by REvil, some ransomware CTAs have engaged in targeting former victims who have already paid ransoms. In these cases, the CTAs request additional payment and threaten to publicly post the same data they allegedly deleted from the first attack after the ransom was paid. In rare cases, the CTAs will still post the data even if the ransom is paid twice.

Exfiltration Techniques

Most ransomware infections begin through a simple initial attack vector, such as a phishing email or exploiting unsecured Remote Desktop Protocol (RDP). After initial access, cybercriminals use malware, open-source penetration testing tools, and living-off-the-land techniques to escalate privileges and move laterally across the victim's network. The increased network access allows CTAs to target critical data for exfiltration and encryption. The typical infection process is depicted below.


Prepares initial attack vector
RDP Citrix
Malspam Spearphish
User clicks on link Infection of first device
Additional malware dropped
Pen testing tools
Living off the land
Lateral movement
Privilege escalation
Data exfiltration
Ransomware dropped
Maximizes damage by encrypting as much data as possible

According to the MITRE ATT&CK Framework, the following techniques are used to exfiltrate data (please see the recommendations section for best practices stemming from these tactics):

- **Automated Exfiltration (T1020):** Using automated methods, such as traffic duplication, to exfiltrate data. Used to streamline sending data from an infected system to a server.
- **Data Transfer Size Limits (T1030):** Used to exfiltrate data in fixed-size chunks rather than as a whole. Commonly used to avoid network data transfer threshold alerts from triggering.
- **Exfiltration Over Alternative Protocol (T1048):** Used as an alternative to exfiltrating data over typical command and control protocols, such as through symmetric, asymmetric, or unencrypted/obfuscated network protocols. Used when CTAs want to send data using an alternative route.
- **Exfiltration Over C2 Channel (T1041):** Exfiltrating data using an existing command and control channel. Most often used to encode the data as normal communications, minimizing outbound connections to avoid detection.
- **Exfiltration Over Other Network Medium (T1011):** Technique used to exfiltrate data through network mediums, such as Bluetooth and Cellular Data. Used if the other network options are inaccessible or not properly geared to exfiltrate data without risk of detection.

- **Exfiltration Over Physical Medium (T1052):** Using physical means of exfiltrating data, such as USB. Most often used as the final exfiltration point or to access disconnected systems.
- **Exfiltration Over Web Service (T1567):** Using a legitimate web service to exfiltrate data. Helps reduce the risk of any suspicious network detections.
- **Scheduled Transfer (T1029):** Used to exfiltrate data at specific times or intervals. Most often used to combine data transfer traffic with normal activity to avoid detection.
- **Transfer Data to Cloud Account (T1537):** When exfiltrated data is transferred from one cloud environment to another and often to avoid risk of network-based exfiltration detections.

Ransomware Variants Using Exfiltration

- **Posting Data On Leak Sites:** Avaddon, Ako, Clop, Conti, Darkside, DoppelPaymer, Egregor, Everest, Lockbit*, Light*, Maze, Mespinoza, MountLocker, Nefilim, Nemty*, Netwalker, Pay2Key, Ragnarok, RagnarLocker, RansomeEXX, REvil, Sekhmet*, Snatch*, Suncrypt [5,6,7,8,9,10,11
- **Posting/Publicizing Data Leaks On Underground Forums:** Avaddon, Ako, Darkside, Egregor, Kupidon, Maze, Nemty, REvil, Sekhmet, Suncrypt [5,6,9,10
- **Publicizing Data Leaks on Twitter:** DoppelPaymer, Maze, RagnarLocker*, Snatch* [5,7,8]
- **Selling/Auctioning data:** DoppelPaymer, Maze, REvil [5,8]
  ** denotes a currently inactive site or Twitter Handle*

Recommendations

The MS-ISAC does not encourage victims to pay the ransom, as it further incentivizes this criminal behavior, but understands this can sometimes be the only available option. Organizations that suffer a ransomware attack should anticipate data exfiltration occurred prior to the ransom note. The MS-ISAC recommends implementing proper data management, behavioral analytics to track access to data, and access controls, paying special attention to the most critical or sensitive data. Actions include mapping the organization’s data spread and structure, properly classifying it, encrypting known sensitive data at rest and in transit, and adhering to the principle of least privilege.

The MS-ISAC also generally encourages SLTTs to implement a defense-in-depth strategy to combat all types of malicious cyber activity, as there is no single magic bullet. Organizations should consider adhering to the CIS Controls, leveraging the CIS Benchmarks, and reviewing MS-ISAC and CISA services. In addition, the MS-ISAC urges SLTTs to reference the dual seal CISA/MS-ISAC Ransomware Guide.

1. Backups
   - Maintaining offline encrypted backups and regularly testing restoral procedures.

2. Incident Response & Communications Plan
   - Create, maintain, and exercise a basic cyber incident response plan and associated communications plan that includes response and notification procedures.

3. Data Sprawl

- Identify and track different types on systems. Catalog all the locations where sensitive data and other intellectual property is stored and who has privileges to access the data. Once complete, implement robust access control policies.

4. Network Segmentation
    - Employ logical or physical network segmentation, separating various business units or departments.

5. Defend against initial infection vectors
    - Malicious emails
        - Implement email filtering.
        - Conduct regular end-user awareness trainings on how to identify and respond to suspicious emails.
        - Implement Domain-based Message Authentication, Reporting and Conformance (DMARC) policy and verification. DMARC builds on the widely deployed Sender Policy Framework and Domain Keys Identified Mail protocols, adding a reporting function for senders and receivers.
    - Remote Access and Internet-Facing Vulnerabilities
        - Conduct regular vulnerability scanning.
        - Regularly patch and update software and operating systems.
        - Secure RDP and other remote desktop services.
    - Managed Service Providers (MSPs)
        - Consider the risk management and cyber hygiene practices of third parties or managed service providers (MSPs) your organization uses. MSPs have been a major inlet for CTAs seeking ransom client organizations.

6. Detection and logs
    - Ensure antimalware software and signatures are up to date. Ensure automatic updates for these defenses are turned on.
    - Consider implementing an intrusion detection system (IDS). The MS-ISAC encourages SLTT organizations to look into procuring and deploying an Albert IDS system to enhance a defense-in-depth strategy. Learn more about Albert here.
    - Consider implementing other detection defenses, such as an intrusion prevention system (IPS) or an Endpoint Detection and Response (EDR) solution.
        - The MS-ISAC is conducting an EDR pilot for SLTT organizations. For more information, please email info@msisac.org.
    - CISA and the Center for Internet Security (CIS) are teaming up with Akamai to provide a Malicious Domain Blocking and Reporting (MDBR) service at no cost to members of the MS-ISAC and EI-ISAC. Sign up for MDBR
    - Baseline and analyze network activity over a period of months to determine behavioral patterns. Distinguishing normal activity from anomalous network activity is a major step in detecting malicious network activity.

MITRE Tactic-Specific Recommendations:

Automated Exfiltration (T1020)

- Use best practices for authentication protocols, such as Kerberos. (Protect Countermeasure)
- Ensure web traffic that can contain credentials is protected via SSL/TLS. (Protect Countermeasure)
- Ensure that all wired or wireless traffic is encrypted appropriately. (Protect Countermeasure)

Data Transfer Size Limits (T1030)

- Deploy network-based Intrusion Prevention Systems (IPS) to block malicious network traffic at each of the organization's network boundaries. (Protect Countermeasure)

Exfiltration Over Alternative Protocol (T1048)

- Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. The machine should not be used for reading e-mail, composing documents, or browsing the internet. (Protect Countermeasure)
    - Create a separate wireless network for personal or untrusted devices. Enterprise access from this network should be treated as untrusted and filtered and audited accordingly.
- Deploy network-based Intrusion Prevention Systems (IPS) to block malicious network traffic at each of the organization's network boundaries. (Protect Countermeasure)
- Decrypt all encrypted network traffic at the boundary proxy prior to analyzing the content. However, the organization may use allow-lists of allowed sites that can be accessed through the proxy without decrypting the traffic. (Detect Countermeasure)
    - Deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary of the network at each of the organization's network boundaries.

Exfiltration Over C2 Channel (T1041)

- Deploy network-based Intrusion Prevention Systems (IPS) to block malicious network traffic at each of the organization's network boundaries. (Protect Countermeasure)

Exfiltration Over Other Network Medium (T1011)

- Maintain standard, documented security configuration standards for all authorized network devices. (Protect Recommendation)

Exfiltration Over Physical Medium (T1052)

- Remove sensitive data or systems not regularly accessed by the organization from the network. These systems shall only be used as standalone systems (disconnected from the network) by the business unit needing to occasionally use the system or completely virtualized and powered off until needed. (Protect Countermeasure)
- Utilize application allow-listing technology on all assets to ensure that only authorized software executes and all unauthorized software is blocked from executing on assets. (Protect Countermeasure)

  - Ensure that unauthorized software is either removed or the inventory is updated in a timely manner.
  - The organization's application allow-listing software must ensure that only authorized software libraries (such as *.dll, *.ocx, *.so, etc.) are allowed to load into a system process.
  - Uninstall or disable any unauthorized browser or email client plugins or add-on applications.

Exfiltration Over Web Service (T1567)

- Restrict use of certain websites, blocking downloads/attachments, blocking JavaScript, restrict browser extensions, etc. (Protect Countermeasure)

Scheduled Transfer (T1029)

- Deploy network-based Intrusion Prevention Systems (IPS) to block malicious network traffic at each of the organization's network boundaries. (Protect Countermeasure)

Transfer Data to Cloud Account (T1537)

- Deploy network-based Intrusion Prevention Systems (IPS) to block malicious network traffic at each of the organization's network boundaries. (Protect Countermeasure)
  - Deny communications with known malicious or unused Internet IP addresses and limit access only to trusted and necessary IP address ranges.
- Use an automated tool, such as host-based Data Loss Prevention, to enforce access controls to data even when data is copied off a system. (Protect Countermeasure)
- Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will help enforce need-to-know policies. (Protect Countermeasure)
- Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities. Disabling these accounts, instead of deleting accounts, allows preservation of audit trails. (Protect Countermeasure)
  - Disable any account that cannot be associated with a business process or owner.

References

[1]: https://blog.chainalysis.com/reports/ransomware-ecosystem-crypto-crime-2021
[2]:https://www.zdnet.com/article/university-of-california-sf-pays-ransomware-hackers-1-14-million-to-salvage-research/
[3]:https://healthitsecurity.com/news/maze-ransomware-hackers-extorting-providers-posting-stolen-health-data
[4]:https://healthitsecurity.com/news/ransomware-hacking-groups-post-data-from-5-healthcare-entities
[5]:https://www.bleepingcomputer.com/news/security/new-avaddon-ransomware-launches-in-massive-smiley-spam-campaign/
[6]:https://www.zerofox.com/blog/team-snatch-data-breach/
[7]:https://bleepingcomputer.com/news/security/doppelpaymer-ransomware-sells-victims-data-on-darknet-if-not-paid/

[8]:https://www.bleepingcomputer.com/news/security/darkside-new-targeted-ransomware-demands-million-dollar-ransoms/
[9]:https://www.bleepingcomputer.com/news/security/nemty-ransomware-to-start-leaking-non-paying-victims-data/
[10]:https://research.checkpoint.com/2020/pay2key-the-plot-thickens/
[11]:https://www.bleepingcomputer.com/news/security/new-avaddon-ransomware-launches-in-massive-smiley-spam-campaign/