Email Collection, Technique T1114 - Enterprise

Archived: 2026-04-05 17:16:17 UTC

Sub-techniques (3)

Adversaries may target user email to collect sensitive information. Emails may contain sensitive data, including trade secrets or personal information, that can prove valuable to adversaries. Emails may also contain details of ongoing incident response operations, which may allow adversaries to adjust their techniques in order to maintain persistence or evade defenses.[1][2] Adversaries can collect or forward email from mail servers or clients.

ⓘ

Platforms: Linux, Office Suite, Windows, macOS

Contributors: Menachem Goldstein; Swetha Prabakaran, Microsoft Threat Intelligence Center (MSTIC)

Last Modified: 24 October 2025

Procedure Examples

Mitigations

ID	Mitigation	Description
M1047	Audit	Enterprise email solutions have monitoring mechanisms that may include the ability to audit auto-forwarding rules on a regular basis. In an Exchange environment, Administrators can use Get-InboxRule to discover and remove potentially malicious auto-forwarding rules.[12]
M1041	Encrypt Sensitive Information	Use of encryption provides an added layer of security to sensitive information sent over email. Encryption using public key cryptography requires the adversary to obtain the private certificate along with an encryption key to decrypt messages.
M1032	Multi-factor Authentication	Use of multi-factor authentication for public-facing webmail servers is a recommended best practice to minimize the usefulness of usernames and passwords to adversaries.

ID	Mitigation	Description
M1060	Out-of-Band Communications Channel	Use secure out-of-band authentication methods to verify the authenticity of critical actions initiated via email, such as password resets, financial transactions, or access requests. For highly sensitive information, utilize out-of-band communication channels instead of relying solely on email to prevent adversaries from collecting data through compromised email accounts.[1]

Detection Strategy

ID	Name	Analytic ID	Analytic Description
DET0476	Email Collection via Local Email Access and Auto-Forwarding Behavior	AN1309	Correlates creation of email forwarding rules or header anomalies (e.g., X-MS-Exchange-Organization-AutoForwarded) with suspicious process execution, file access of .pst/.ost files, and network connections to external SMTP servers.
		AN1310	Detects file access to mbox/maildir files in conjunction with curl/wget/postfix execution, or anomalous shell scripts harvesting user mail directories.
		AN1311	Monitors Mail.app database or maildir file access, automation via AppleScript, and abnormal mail rule creation using scripting or UI automation frameworks.
		AN1312	Correlates unusual auto-forwarding rule creation via Exchange Web Services or Outlook rules engine, presence of X-MS-Exchange-Organization-AutoForwarded headers, and logon session anomalies from abnormal IPs.

References

1. Tyler Hudak. (2022, December 29). To OOB, or Not to OOB?: Why Out-of-Band Communications are Essential for Incident Response. Retrieved August 30, 2024.
2. CISA. (2021, April 15). Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations. Retrieved August 30, 2024.
3. Microsoft Threat Intelligence. (2023, June 14). Cadet Blizzard emerges as a novel and distinct Russian threat actor. Retrieved July 10, 2023.
4. US Cybersecurity & Infrastructure Security Agency et al. (2024, September 5). Russian Military Cyber Actors Target U.S. and Global Critical Infrastructure. Retrieved September 6, 2024.
5. CIS. (2018, December 12). MS-ISAC Security Primer- Emotet. Retrieved March 25, 2019.
6. Kessem, L., et al. (2017, November 13). New Banking Trojan IcedID Discovered by IBM X-Force Research. Retrieved July 14, 2020.
7. Binary Defense. (n.d.). Emotet Evolves With new Wi-Fi Spreader. Retrieved September 8, 2023.
8. Certfa Labs. (2021, January 8). Charming Kitten’s Christmas Gift. Retrieved May 3, 2021.
9. CISA. (2023, November 16). Cybersecurity Advisory: Scattered Spider (AA23-320A). Retrieved March 18, 2024.
10. DOJ. (2018, March 23). U.S. v. Rafatnejad et al . Retrieved February 3, 2021.
11. Park, S. (2024, June 27). Kimsuky deploys TRANSLATEXT to target South Korean academia. Retrieved October 14, 2024.
12. McMichael, T.. (2015, June 8). Exchange and Office 365 Mail Forwarding. Retrieved October 8, 2019.
