The Poisoned Postman: Detecting Manipulation of Compliance Features in a Microsoft Exchange Online Environment

Rebel Powell

The Poisoned Postman: Detecting Manipulation of Compliance Features in a Microsoft Exchange Online Environment

GIAC GCIH Gold Certification

Author: Rebel Powell, rebelpowell@gmail.com
Advisor: Lenny Zeltser

Accepted: August 23, 2020

Abstract

Modern attack techniques frequently target valuable information stored on enterprise communications systems, including those hosted in cloud environments. Adversaries often look for ways to abuse tools and features in such systems to avoid introducing malicious software, which could alert defenders to their presence (Crowdstrike, 2020). While on-premise detection strategies have evolved to address this threat, cloud-based detection has not yet matched the adoption pace of cloud-based services (MITRE, 2020). This research examines how adversaries can perform feature attacks on organizations that use Microsoft Office 365's Exchange Online by exploring recent advanced persistent threat tactics in Exchange on-premise environments and applying variations of them to Exchange Online's Compliance and Discovery features. It also analyzes detection strategies and mitigations that businesses can apply to their systems to prevent such attacks.

1. Microsoft Exchange and Exchange Online – A Strategic Target

Though business communication platforms continue to innovate with technologies like instant messaging and chat services, no method dominates the professional communication spectrum more than email. In a four-year communications study from 2016-2020, the technology market research firm The RadiCati Group identified that 64% of businesses still use email as a primary form of communication, and the group projected a 4.3% growth in the trend in 2021 (The RadiCati Group Inc, 2020). Email services are used to communicate sensitive business data, including strategies, private data, and intellectual property. Many small and medium-sized businesses have also moved this vital function to cloud-hosted environments like Microsoft's Exchange Online to increase availability and reduce costs. In their 2019 Cloud Adoption report, Cloud Access Service Broker BitGlass highlighted the exponential adoption of one particular environment - Microsoft's Office 365 Productivity Suite (including Exchange Online in the Enterprise Licensing Tier) which accounted for a 79% market share, overtaking Google's G-Suite after a three-year adoption battle (BitGlass, 2019).

Advanced Persistent Threat (APT) groups have long recognized the strategic value of obtaining covert access to these business email communication systems to enable long-term objectives and have increased their capabilities and tactics to address the cloud-adoption trend of potential victims. These groups, differentiated from traditional attackers by their resources and specialized tooling (Leydon, 2020), value strategic operations such as the collection of communications instead of hit-and-run styled malware attacks targeting immediate monetary gain. One particularly aggressive growth trend observed in APT on-premise cyber collection operations is that of utilizing native functionality and system tools to achieve tactical objectives, reducing the attackers' footprint while increasing the difficulty of detection by victims. Dubbed living-off-the-land (LOL) tactics, these attacks accounted for 40% of compromises observed in Crowdstrike's 2019 Global Threat Report, and at least 15% of the LOL attacks targeted email systems (Crowdstrike, 2019). This style of tactic has also been modified for cloud environments where instead of using native executable files on operating systems,

attackers manipulate built-in features and application programming interfaces (APIs) exposed by providers, reducing their footprint in a cloud-based intrusion. While feature abuse tactic reporting on cloud-specific incidents is often rare due to attribution fears by businesses (FBI iC3, 2016), two published on-premise APT incidents give example insights into how capable and advanced Microsoft Exchange native exploitation threat tactics are.

In 2019, ESET researchers exposed APT28's LIGHTNEURON backdoor which used rootkits and steganography to communicate over compromised Microsoft Exchange Mail Transfer Agents (MTAs) while it abused native-Exchange rule functionality to exfiltrate, redirect, or alter victim emails based on specific criteria in on-premise and hybrid-cloud Microsoft Exchange environments (Faou, 2019). The backdoor itself may not have been a native feature abuse capability, but the rules it applied to MTAs made it particularly challenging to detect for victims who were often not auditing the native MTA element of their email systems and are a textbook example of living off the land. This same type of native email server functionality exploitation was also observed by FireEye's 2018 analysis of APT35, who created malicious email forwarding rules abusing Exchange PowerShell functionality in attacks in both on-premise and cloud-hosted Microsoft environments in the financial sector (FireEye, 2018).

A significant risk consideration for small- and medium-businesses who adopt Microsoft Exchange Online environments for business communications relates to their email system's defensibility and audibility. While adversary attacks, tooling, and interest in Exchange environments are undeniable, very little public guidance or standards exist to detect or defeat adversaries in this space. MITRE's specific Microsoft Office 365 ATT&CK matrix, for example, only includes one recognized technique (Email Collection) with three sub-techniques (local collection, remote collection, and email forwarding rules) and provides only generic log review suggestions to combat them (MITRE, 2020). This lack of defensive strategies is attributable to an absence of reporting by victims of adversary tactics but also by a lack of administrator visibility and knowledge of Microsoft Exchange Online environments. A LogicWorks 2020 Survey identified that 86% of respondents identified that cloud engineers' lack of vendor-specific

cloud knowledge would significantly impact their cloud-hosted environment adoption (LogicWorks, 2020). Business adopters and administrators can better protect crucial data that resides in and flows through their email systems and reduce the overall risk of compromise in a quantitatively demonstrable manner by becoming more aware of adversary interests and intent to exploit them.

2. Exchange Online in Action

2.1. Office 365 License and Tool Considerations

Microsoft's Enterprise Office 365 license tiering is available in three offerings – E1, E3, and E5, with costs per-user and features available increasing as the offering's number does. This work considered an E3 and E5 tenet for threat modeling due to the advanced Microsoft Compliance Center and associated tools only being available to those tier-levels. It ultimately proceeded with the E5 tier as it was the only option that included Advanced Compliance features (including eDiscovery 2.0). Small- and medium-sized businesses should similarly identify their needs and choose a tier that meets their minimal compliance and regulatory requirements but should bear in mind that defensive tools and advanced logging are usually only provided in higher license tiers.

Included in the E5 tier are two critical features for adversaries to capitalize upon and for defenders to configure and audit to prevent their success:

- Litigation Hold
- Advanced eDiscovery

Both features are explored in detail in Section 2.3.2. Each features' native functionalities are to enable administrators to collect emails and data from mailboxes that may be involved in legal proceedings where evidence collection and preservation are crucial to investigation and discovery. As APT28 and APT35 have demonstrated, however, they are powerful tools that can also be co-opted to collect data on target victims or entire organizations. Both features and the myriad of other tools available to administrators in Exchange Online are available via a web GUI or a PowerShell add-on applet.

2.2. SANS Swell Sodas Inc.

To fully explore defensive scenarios involving the manipulation of compliance features in an Exchange Online environment, and to qualitatively and quantitatively measure the results of countermeasures put in place, a representative (yet fictional) medium-sized business was created and replicated in a fully functional Microsoft Office 365 E5 Tenet to facilitate the remainder of this research. This entity, SANS Swell Sodas, Inc., represents the more than 79% of businesses that employ between 100-500 users and who are the heaviest users of the Microsoft Office 365 platform (Cole, 2016). Of that group of businesses, 61% list Microsoft Exchange Online as the primary application they use on the Office 365 platform, second only to the file storage service OneDrive. Exchange Online mirrors this trend for the business and provides SANS Swell Sodas their primary communication channel both internally and for contact with external organizations, making it a crucial asset to secure in their cybersecurity plan.

Like 70% of small- and medium-sized businesses, SANS Swell Sodas hosts their most sensitive data in their Microsoft Exchange Online tenet (Proofpoint, 2015). Much of this data storage is unintentional, often resulting from executives or employees emailing each other attachments or documents containing proprietary or competitively valuable information and being unaware of the data being retained in the cloud indefinitely. Further exposing the business to risk, while the email is encrypted in transit via TLS, SANS Swell Sodas has opted not to utilize the data classification and loss prevention capabilities of their Office 365 E5 tenet. This choice mirrors 88% of the small- and medium-size businesses industry who have the same configuration (Cole, 2016). This setup potentially exposes SANS Swell Sodas' most valuable piece of intellectual property – their prize-winning soda recipe, to an attacker whose goal is to capitalize on these weaknesses and exfiltrate the proprietary data for nefarious use.

A final consideration for the SANS Swell Sodas Exchange Online ecosystem is the human element of risk involved. In addition to traditional user email threats like phishing and financial whaling, which must be defended, SANS Swell Sodas only employs five administrators to administer their Exchange Online tenet. These administrators have the cloud-specific knowledge gaps addressed in Section 1, but more importantly, they also represent the more than 64% of Office 365 administrators who have other business-

critical IT duties that do not include administering the email tenet full-time. This demand is reflected in the administrators' schedule, which only allows them to log in to the tenet a few times a week to troubleshoot major issues or to collect logs when required by regulatory necessity.

With the SANS Swell Sodas Inc. Exchange Online environment and its vulnerabilities defined, the business is ready to analyze potential native feature abuse tactics in the environment and to identify qualitative and quantitative controls that can be enacted to reduce the effectiveness of those tactics. Two likely attack paths will be explored to facilitate this implementation, first in the environment using the default configuration of Exchange Online and then with compensating controls enacted. After impact is measured from the controls, they will be aligned to a more extensive continuous monitoring program that is usable by a small- to medium-sized business while considering challenges such as the lack of dedicated administrator resources they have available.

2.3. Attacking SANS Swell Sodas, Inc. – Default Artifacts

With adversary intent, likely targeted attack paths, and a “victim” medium-sized business environment all being developed, analysis of the attacks was conducted and measured for an organization in two differing security postures. The ultimate goal of this study was to develop an effective and repeatable framework to detect and defeat an attacker in an Exchange Online Environment using feature abuse tactics.

2.3.1. The Scenario

Email traffic was generated to act as a collection target for the simulated attacker to create a realistic environment that would act as a baseline for the measurements of defensibility and detectability of an adversary operating in the Exchange Online environment manipulating Compliance features. Using the SANS Swell Soda Inc. E5 tenet described above and the Microsoft Exchange REST API, 543 emails were sent between fifteen employees created in the Office 365 tenet. A significant majority of these messages (71%) contained simulated traditional employee-to-employee daily communications that would have limited value if collected by an adversary. These emails were randomly generated by utilizing a business word dictionary and a Python utility,

Faker (Faraglia, 2020), which outputted random combinations of words from the dictionary to form the body of the messages. The remaining 29% of manually-created emails contained detailed information that SANS Swell Sodas would want to keep out of competitor's hands to maintain their competitive advantage (financial data, PII, etc.), but only three emails held their most valuable intellectual property – their soda's secret recipe.

From the business detection perspective, Exchange Online's default logging settings were utilized with no additional configuration being applied, representing the adoption settings of those in the previously mentioned Skyhigh Networks report. While Microsoft notes that default logging actions are always being updated, changed, and rolled out to E5 tenets (Microsoft 2020), in general, default logging of mailboxes includes basic mail flow data, ownership changes of the mailbox, permanent deletion of messages, and delegation (using the "Send As" feature). An exact listing of audited default functionality during the analysis period was retrieved with various versions of the following PowerShell commandlet:

```
Get-Mailbox <mailbox> | Format-List DefaultAuditSet
```

External access logs (those representing connection source IPs to the Office 365 tenet) were also left with the default configuration enabled.

To create a simulated administrator-level target for the attack, one account (Richard Augustus) was created with the highest privilege level – Global Administrator. This role, which has full administrative purview over Exchange Online and the SANS Swell Sodas Inc. Office 365 E5 tenet has many options and tools available that are not enabled for regular users. Most of these features and privileges exceed the needs of this research; however, two are particularly relevant – Compliance/Discovery Management and Organization Management. When combined, these roles present the Global Administrator the ability to view and download log-files, change or bypass audit logging requirements, and emplace Litigation and Advanced eDiscovery-type holds for all employees of SANS Swell Sodas.

While Microsoft recommends tightly restricting control to these accounts and enforcing security best practices such as multi-factor authentication to access them, multiple 2019 Compromise Analysis Reports from the US Department of Homeland

Security repeatedly underscore that these features are not commonly enabled in victim organizations (DHS, 2019). DHS does not provide exact statistics on the prevalence of the configuration issues with third-party organizations aided in incident response as a privacy consideration, but they do note an "...increasing mix of configurations which have lowered several organizations' cloud security postures." (DHS, 2019).

For the analysis scenario, an adversary was assumed to have compromised the Global Administrator account because of this type of misconfiguration. This compromise was assumed to come as the result of credential stuffing, where a compromise of a third-party service reveals a legitimate password, which is then reused by the Global Administrator for the Office 365 tenet. A 2019 SANS Spotlight, co-sponsored by Microsoft, highlights this type of compromise as one of the most common in Office 365 Instances (Bromiley, 2019). A crucial point to also highlight is that the compromiser in this analysis was an APT-styled adversary, rather than a casual attacker. This changed the goal of the attacker's perspective post-compromise to persistence and continued strategic access instead of a desire exfiltrate data quickly. This persistence is usually achieved in the span of months to years versus hit-and-run style attacks, which operate in times from days to weeks (Crowdstrike, 2020) and focused the attacker's goal on using the Compliance Features to obtain strategic information.

2.3.2. Default Configuration Results – Limited Visibility and Traceability

As emails were sent throughout the Exchange Online instance, manipulation of the two compliance features (Litigation Hold and Advanced eDiscovery) occurred via the compromised Global Administrator account from the adversary perspective. After each of the features was manipulated, a forensic collection on the tenet was taken via PowerShell or via the Exchange Online web GUI (whichever exposed the logs in the most user-friendly method) from the defender perspective to account for the SANS Swell Sodas Administrator's busy schedule and lack of complete knowledge of the Office 365 E5 tenet.

Feature 1: Litigation Hold

As one of the original legal-discovery features introduced in Microsoft Exchange 2007, Litigation Hold (sometimes expanded to include a similar feature known as In-

Place Hold) represents one of the earliest Exchange-specific tools to address litigation requirements. Throughout the feature's evolution, Microsoft has added increasing abilities to select and export entire inboxes, specific emails, or particular message traits to prevent them from being deleted by a user whose mail might be involved in a legal proceeding, preserving evidence for the duration of an investigation. This feature is also one of the most commonly deployed legal retention strategies, with over 56% of businesses having used the tool in either an on-premise Exchange or hosted Exchange Online Environment (Fraizer and Zohlen, 2017). This long-term use of Litigation Hold can be attributed to the age of the feature and use by email administrators for many years and is still supported today in Office 365 tenets. As filtered emails or inboxes which have had Litigation Holds applied are transported or deleted, Exchange creates an immutable version of the email for export to an external Outlook file format – a PST file. This file is then downloaded from the Exchange server to an external storage medium and preserved until the In-Place hold has been deleted. A Microsoft diagram explains this logic in more detail in Figure 1.

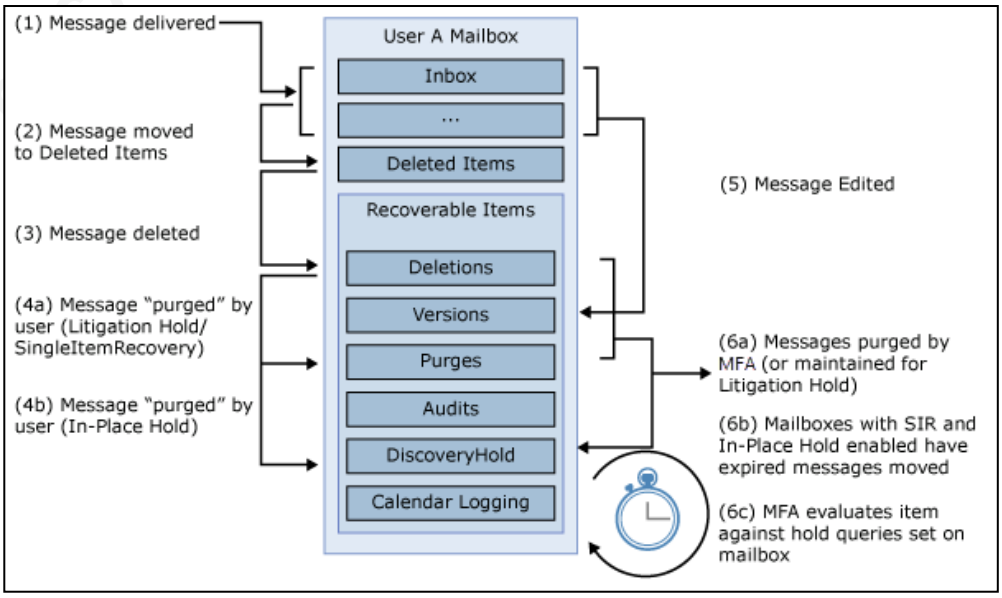


Figure 1. Litigation Hold Preservation/Storage Process (Microsoft, 2019)

From an adversary perspective, Litigation Hold represents a reliable capability to search for and store strategic emails of interest for later export without maintaining an interactive command-and-control of a compromised Exchange server or environment,

which is especially attractive for adversaries. With a one-time compromise and emplacement of the hold, collection can occur for an infinite period, only requiring an adversary to return to collect the final product. This attack reduces the victim detection capability to viewing only audit logs if their tenet was configured to collect them. Combined with the 90-day default log retention period highlighted in Section 1, compromised Litigation Hold makes detection by a victim with a limited security staff extremely challenging.

In the first quarter of 2020, Microsoft announced the retirement of the Litigation Hold feature in Exchange Online in favor of the more Advanced eDiscovery suite of compliance tools (Microsoft. 2020). However, this research highlights Litigation Hold as still an unusually highly usable abuse tactic because of its phase-out methodology. After July 1, 2020, new Litigation Holds are no longer creatable via the web GUI or Exchange PowerShell. After October 1, 2020, only deleting Litigation Holds from the Exchange PowerShell is possible. This time window of opportunity presents the adversary an ideal LOL scenario where they could enable a Litigation Hold before the July 1 date in a compromised tenet, have it become graphically undetectable by a GUI-focused victim administrator, and only become discoverable after October via PowerShell analysis if the log retention was appropriately configured. This phase-out offers Litigation Hold as a very likely exploitation opportunity by an adversary with a uniquely created blind-spot for victims who may be unaware of the tactic and deprecation timeline.

Feature 1 Key Observations

Key observations from the Litigation Hold forensic collection in the default configuration of Exchange Online call attention to the extreme difficulty of detecting an attacker compromise where this living off the land attack is utilized. To simulate the adversary living off the land with this feature, a Litigation Hold was created with the search query “recipe” and applied to all mailboxes on the SANS Swell Sodas tenet. This resulted in another employee (Jasmin Smith) being discovered as the only worker with an email containing the keyword and allowed a subsequent targeted Litigation Hold to be placed on her mailbox (see Figure 2). Visually, the only administrator indication of the hold was a single text entry in the Litigation and In-Place Hold sub-menu of the

Exchange Online Control Panel (requiring eight clicks to discover). This artifact was also able to be queried via the following PowerShell commandlet:

```
Get-Mailbox <mailbox> | LitigationHold*
```

In both cases, only a single line entry explaining the hold (which was filled in with an innocuous comment from the attacker) provided information about the hold.

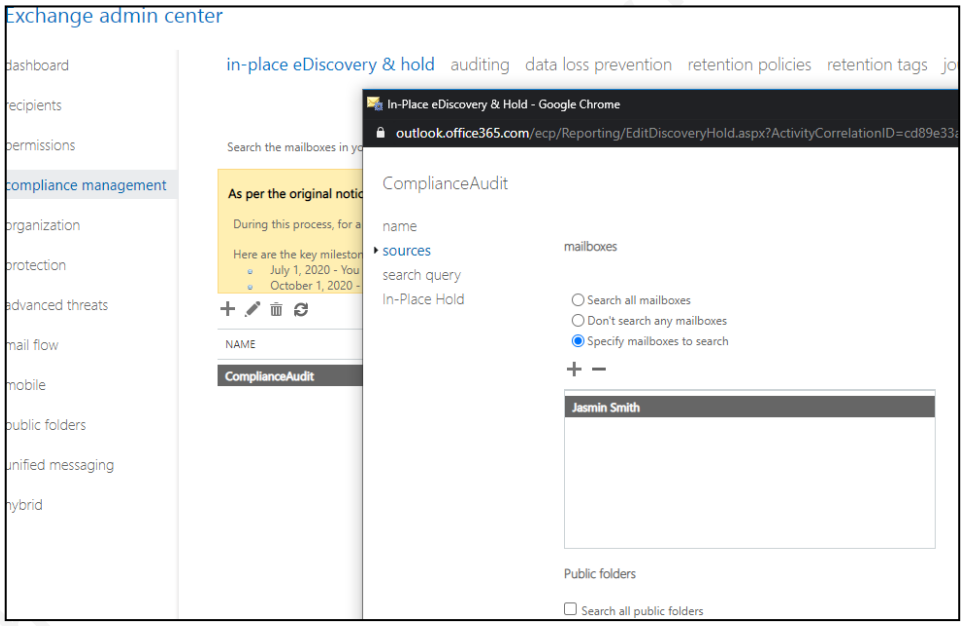


Figure 2: Targeted Litigation Hold via the GUI

With the default logging configuration enabled, only six log artifacts related to the Litigation Hold tactic were discoverable via examination of two logs. These logs, which had analysis complicated by unintelligible GUIDs and SIDS generated by the Exchange Tenet itself, showed that the compromised administrator had accessed the victim's mailbox and created a Litigation Hold. Details regarding the filters used or result achieved were not noted in the logs examined with the default configuration enabled, meaning discovery without further interviewing the staff involved to note the discrepancy would prove perplexing. An example audit log is shown in Figure 3 for further review.

```
  <Event Caller="Arbitration_c1d3d73a-0a1d-4cb2-ba17-
715b9c37fe19@sansswellsodas.onmicrosoft.com" Cmdlet="Set-MailboxSearch" RunDate="2020-
06-26T23:07:49+00:00" Succeeded="true" ExternalAccess="false"
OriginatingServer="BYAPR02MB3976 (15.20.3131.023)" ClientIP="53.23.98.112:27814">
    <CmdletParameters>
      <Parameter Name="InPlaceHoldEnabled" Value="True" />
      <Parameter Name="Name" Value="Compliance" />
      <Parameter Name="Identity"
Value="ODcwMzI4MTItODg0Mi00MWYxLWE4ZmYtYzE0NDQ1YjQ4ZDE1XDdhYTUyOWYxLTYwMjktNDM0NS1hOTU3
LWEzMDgxZjQ1MGZiOA2" />
    </CmdletParameters>
```

Figure 3: In-Place Litigation Hold Trace Log

The tactic was also effective for the adversary's goal, quickly locating the one email in the entire tenet meeting the search criteria. This email was transparently archived based on the Litigation Hold's disposition with no indication to the recipient. Exfiltration of the resulting 56KB PST archive took less than two minutes. It resulted in only one additional export log event being created in the Exchange Administrator Audit log, making the Litigation Hold tactic a high-impact and low-traceable one in SANS Swell Sodas' default configured E5 tenet.

Feature 2: Advanced eDiscovery

The Advanced eDiscovery (sometimes known as strictly eDiscovery 2.0) is the improved litigation and compliance solution, which will fully replace Litigation Hold in Exchange Online tenets in 2020 (Microsoft, 2020). As a component of the overall Microsoft Compliance ecosystem of tools, Advanced Discovery targets the entire corporate litigation workflow of tenet data rather than just the technical email artifacts. Improvements include better indexing features for searchability, document tagging, visible dashboards, and a case-centered view of investigation(s) in progress. An example use of this ligation workflow is shown in Figure 4.

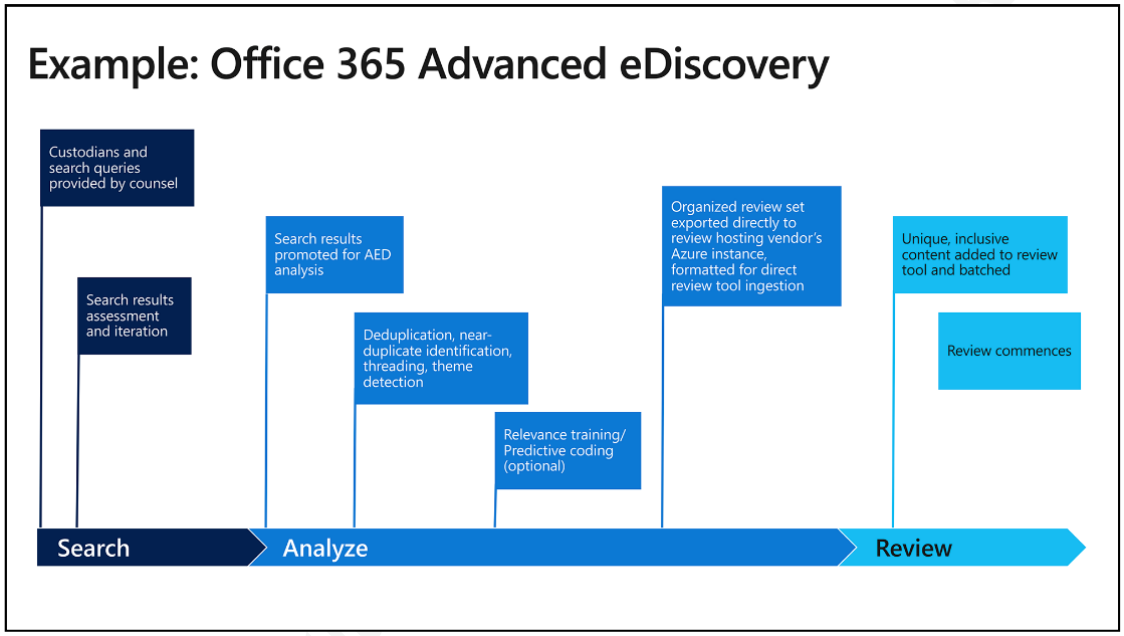


Figure 4. Advanced eDiscovery Litigation Workflow (Microsoft, 2019)

With these advanced feature introductions come an increased attack surface for potential adversaries looking to live off the land in Exchange Online. In their 2020 Microsoft Office 365 License Optimization Report, SaaS Provider CoreView discovered that of companies using E5 licensed tenets, 38% could reduce their license to the E1 tiers based on their lack of use of the E5 feature set. However, many of these companies cannot do so because they adopt E5 tenets for specific features only available at that license level, such as the Microsoft Advanced Threat Protection (ATP) security program (Coreview, 2020). Companies in this adoption pattern lack knowledge or necessity to utilize extra features available to them. This "no-person's-land" of unused features is where attackers gain another likely Exchange Online native feature abuse tactic.

By utilizing new indexing features available in Advanced eDiscovery against Exchange Online tenets, attackers can more tightly focus data selection for exfiltration from a compromised victim while maintaining a much smaller footprint in the organization. The adversary data collection net has also been expanded to include file metadata, email importance level, and even conversations from Skype for Business and Microsoft Teams (which are stored in Exchange Online). As a final challenge for detection during the exfiltration stage, cases from Advanced eDiscovery are exportable to

the victim's Azure Cloud storage tenet or an adversary procured Azure storage blob (Microsoft, 2020) for download, further obfuscating potential infrastructure involved without additional logging being enabled pre-compromise. More attack surfaces are also exposed for the small- or medium business' larger Office 365 tenet by Advanced eDiscovery, but these scenarios exceed the scope of this research. The Future Implications section and Microsoft's own Advanced Security Reference best outline further threat modeling potential.

Feature 2 Key Observations

The Advanced eDiscovery abuse tactic proved equally effective against the default Exchange Online logging configuration. After beginning the attack on a separate day to minimize cross-logging contamination from the Litigation Hold (Microsoft does not allow clearing of the Exchange Online log entirely), a similar search was conducted on SANS Swell Sodas' tenet. However, this tactic was enabled via a separate and more detailed GUI – the Microsoft Compliance Center, which is a separate component from the Exchange Online Control Panel. While the results were much more visible graphically to the victim in the Compliance Center (showing as a large "1" in the Number of Cases), there were no visual indicators created in the Exchange Online Control Panel concerning the search, requiring the SANS Swell Sodas Administrators to be looking at a different interface to detect the intrusion.

When combined with the previously discussed lack of administrator knowledge presented by LogicWorks, SANS Swell Sodas faces a high likelihood that this tactic would go undetected. Specifically, detection of the Advanced eDiscovery presented key challenges, requiring both:

- An administrator to have a specific need to check the Compliance Center during the attack.
- Knowledge of Auditing/Compliance Logs and Compliance Center Logging Locations.

Exfiltration from the Compliance Center was also more complicated when compared to the Litigation Hold from an adversary perspective, but because it utilized Microsoft native features via Azure storage blobs, it also became much more complicated to detect

(requiring knowledge of Blob ID ownership to fully trace). With less than half the artifacts of the Litigation Hold tactic and the additional difficulty in acquiring them, the Advanced eDiscovery tactic proved extremely efficient and difficult to detect or prevent with default configurations enabled.

Feature Manipulation Results – Default Configuration

In summary, both the Litigation Hold and Advanced eDiscovery feature abuse tactics proved effective for the medium-sized business lacking dedicated Exchange Online resources to detect or prevent in an Exchange Online E5 tenet with a default configuration applied. The table below summarizes and scores critical elements from each tactic. They include:

- The number of artifacts generated
- The ease of accessing these artifacts
- The likelihood that the artifact would lead to the successful detection of the tactic

Scores are scaled from one to five, with one being the easiest to access and five being the most difficult. For detection, one represents the easiest to detect, and five is the least likely to be detected. A final observation for this phase is the score of the Advanced eDiscovery on Likelihood of Detection – this score is adjusted to address that if SANS Swell Sodas were able to locate the Compliance logging, they would be highly likely to discover that the tactic was deployed.

Tactic	Artifacts Created	Accessibility of Artifacts	Likelihood of Detection
Litigation Hold	6	3	2
Advanced eDiscovery	3	5	3

Figure 5: Detection Success Matrix in Default Configuration

3. Protecting the Secret Recipe – Improving Detection

With the viability of two adversary potential attack paths demonstrated and the difficulty of administrator detection being made evident, the second phase of the analysis shifted focus to increasing the likelihood of detection and prevention by increasing the victim administrator's knowledge of features available in E5 tenets. By aiding potential victims to use the same living off the land methodologies in Exchange Online from a defensive perspective, this phase determined two effective techniques that can be enacted to combat an attackers' ability to operate stealthily in their environment. Given the increasing availability of tools in the Office 365 ecosystem, advanced study of each tool's effectiveness would not be practical. However, the techniques chosen demonstrate low-difficulty to implement and high-impact countermeasures that small and medium-sized businesses can deploy quickly to increase visibility.

3.1. Logging Architecture and Artifacts

As adoption of Office 365 by organizations with strict compliance and reporting requirements has increased, so too have Microsoft's auditing capabilities, especially those of privileged accounts. The bulk of this research will examine two particular logs for artifacts: the Exchange Trace Logs and the Audit Log in the Security and Compliance Center. Both logs include multiple indicators of an administrator or potential adversary activity when examined by a business, especially when their Office 365 hosted tenet is configured with advanced logging capabilities enabled. This is a recommendation discussed in Section 4. A detailed overview of the logging infrastructure and its positioning within the Microsoft Office 365 and Exchange Online ecosystem is illustrated in Figure 6 below.

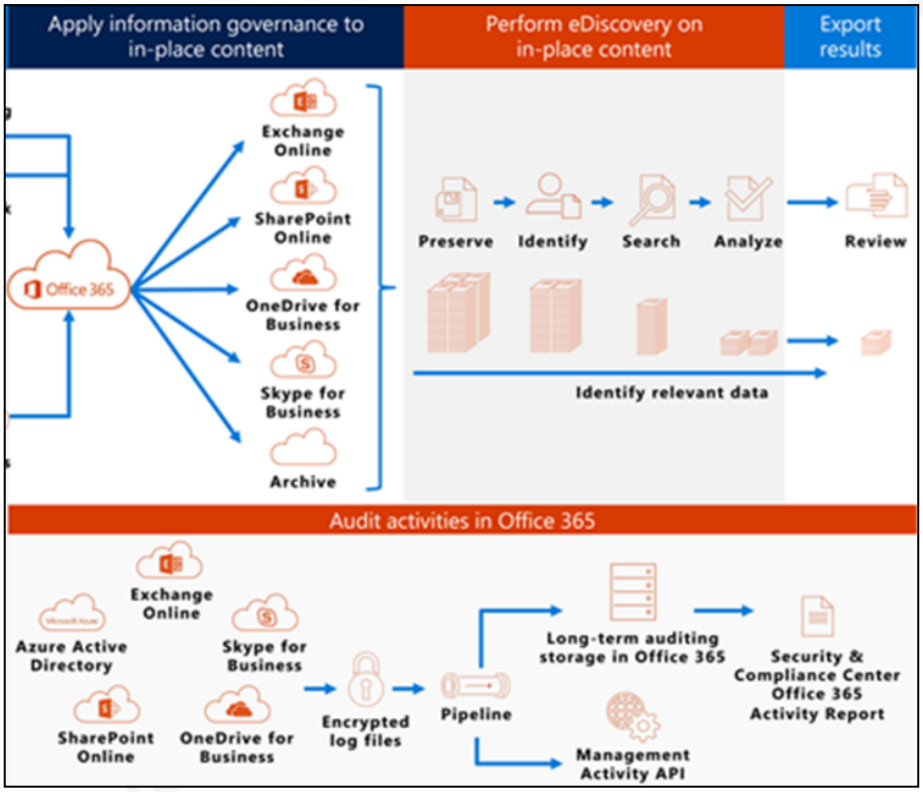


Figure 6. Audit Activities and Governance in Office 365 (Microsoft, 2019)

Email inboxes or individual messages manipulated by the Litigation Hold or eDiscovery features are selected from the mail stream based on rules designed by administrators via the GUI or management PowerShell and are held in resulting mailboxes. These rules can be as simple as "select all emails to and from rrositas@sansswellsodas.com" or much more specific based on content such as "hold any email with an attachment file that is a docx file with a filename containing recipe." This wide variety of filtering enables organizations to minimize over-selecting emails, which could have fiscal implications for increased storage requirements or liability implications for potential violations of reasonable privacy expectations. To aid in repudiation and chain-of-custody questions on what rules were enacted by which administrator, detailed audit trails are written to logs stored in Office 365 and accessed via the Management Activity API.

Logging in Office 365 is critical to a business defending against adversaries attacking using native features. However, a critical knowledge requirement for

administrators and adopters is that logs are sometimes limited or nonexistent based on where features are accessed. An example of this can be seen in the eDiscovery Audit Log, which only includes tasks configured from the Compliance Center. If performed from the Exchange Online Portal, those same activities would NOT be logged in the Audit Log (Microsoft, 2020). Additionally, logging is not enabled by default for most Office 365 features, and log retention is by default set to 90 days maximum. Microsoft has indicated plans to address this lack of logging threat but has not set a firm timeline for implementation.

Mitigation 1: Advanced Logging and Unified Log Review

Logging is one of the most fundamental elements required to investigate an intrusion involving a potential adversary compromise. Properly configured logs enable an analysis of campaign timelines, artifacts left by the attacker, successful exploitations of misconfigurations, and provide insight into the ultimately targeted information. In Exchange Online and Microsoft Office 365, however, logging is configured by default to consider fiscal implications on storage space rather than from a defensive perspective (Microsoft, 2020). Though Microsoft continues to improve their logging default settings for Office 365, depending on the year a tenet was purchased or migrated to, disparate settings may be encountered. An example of this can be seen in the Mailbox Auditing examined in Section 3's artifact samples. Since January 2019, Mailbox Auditing has been enabled by default in new Microsoft Office 365 E5 tenets. However, tenets purchased before this date may have lower Mailbox Auditing verbosity enabled or even no Mailbox Auditing at all enabled.

To combat potential verbosity issues with Mailbox Auditing logging or allowing non-standard logging configurations like those analyzed by DHS from being operated, businesses should enable logging to the best level of verbosity available while still respecting their cloud storage budget (DHS, 2019). While this quota will be different for each organization, Microsoft and DHS both recommend ensuring verbose Mailbox Auditing for all mailboxes in the organization is enabled. To apply this recommendation to the analysis of SANS Swell Sodas Inc., the following DHS recommended PowerShell commandlet was issued:

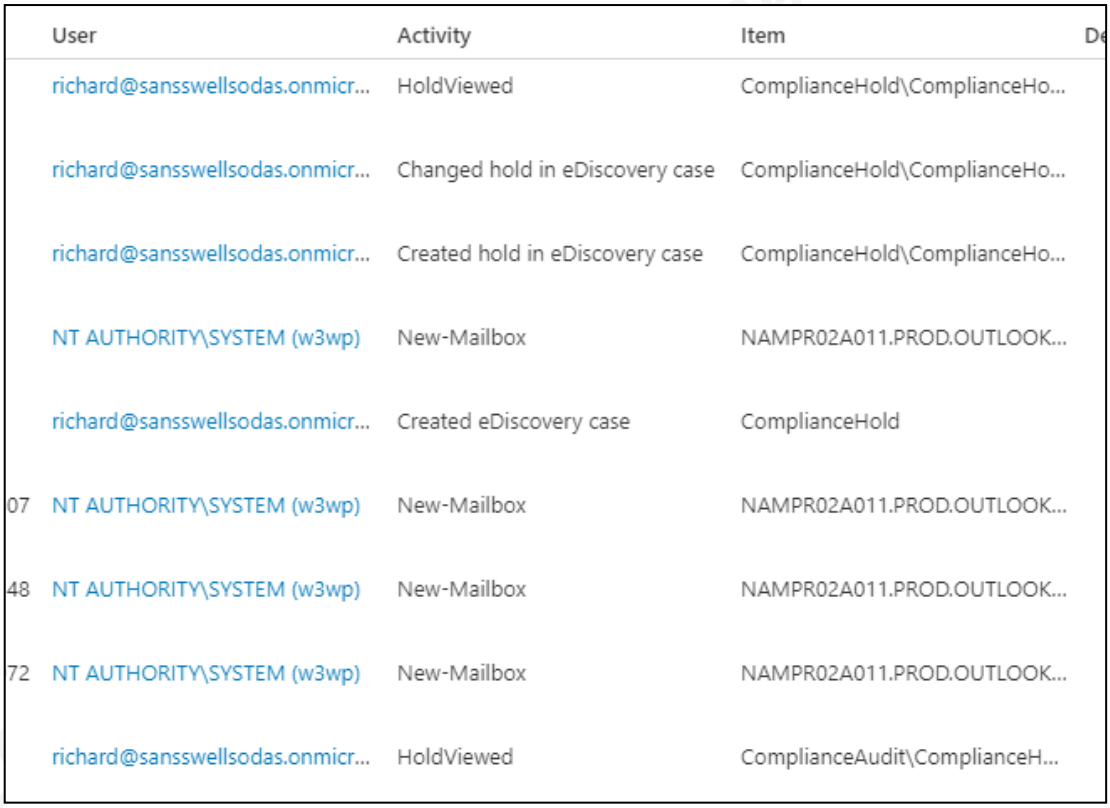
```
Get-Mailbox -ResultSize Unlimited | Set-Mailbox -
AuditEnabled $true -AuditOwner
MailboxLogin,HardDelete,SoftDelete,Update,Move -
AuditDelegate SendOnBehalf,MoveToDeletedItems,Move -
AuditAdmin Copy,MessageBind
```

Mitigation 1 Key Observations

This command resulted in a more coherent and detailed audit log, which allowed Litigation Hold-type feature attacks to drastically increase the number of artifacts created on all mailboxes in the SANS Swell Soda tenet and increased the speed of log analysis by investigators while only increasing storage utilization by 11%. A marked improvement in the analysis investigation occurred with the increased verbosity enabled. Details relating to each time a Litigation Hold query was run against the organization were logged, and each mailbox noted a "non-owner mailbox accessed" event in the new logs. With the same attacker queries from the first phase of the analysis, this created 45 events in two minutes, significantly improving the likelihood a victim administrator would recognize automated reconnaissance against their tenet in a log review. A full list of all audit logs enabled via this command is available in the Appendix.

A final pair of considerations for logging to combat adversary native feature attacks in a small- to medium-sized business Exchange Online environment is both the retention time and log review policy enacted by the organization. As mentioned in Section 2, Microsoft's default setting for log retention is 90 days (Microsoft, 2020). This retention covers a basic level of logging (including Mailbox auditing) but also excludes relevant invents in an attacker compromise (such as access to the Azure tenant from Exchange Online used to select victim mailboxes to query with Compliance features). By creating a new retention policy that mirrors most organizations' on-site one-year requirement (Proofpoint, 2015), potential victims increase their opportunity of detection timeline and their ability to remove an emplaced adversary in their infrastructure by having the ability to review each action taken by the attacker after the initial compromise. Logs can now also be reviewed in the Unified Log application in the Microsoft Compliance and Trust Center (Figure 7). This log review process alleviated two difficulties highlighted in the

Advanced eDiscovery tactic from Section 3 – a lack of log location knowledge and the detail contained within the log. This Unified Audit Log shows a much more understandable chain of events from the attacker's reapplied tactics after the settings were enabled.



	User	Activity	Item	De
	richard@sansswellsodas.onmicr...	HoldViewed	ComplianceHold\ComplianceHo...	
	richard@sansswellsodas.onmicr...	Changed hold in eDiscovery case	ComplianceHold\ComplianceHo...	
	richard@sansswellsodas.onmicr...	Created hold in eDiscovery case	ComplianceHold\ComplianceHo...	
	NT AUTHORITY\SYSTEM (w3wp)	New-Mailbox	NAMPR02A011.PROD.OUTLOOK...	
	richard@sansswellsodas.onmicr...	Created eDiscovery case	ComplianceHold	
07	NT AUTHORITY\SYSTEM (w3wp)	New-Mailbox	NAMPR02A011.PROD.OUTLOOK...	
48	NT AUTHORITY\SYSTEM (w3wp)	New-Mailbox	NAMPR02A011.PROD.OUTLOOK...	
72	NT AUTHORITY\SYSTEM (w3wp)	New-Mailbox	NAMPR02A011.PROD.OUTLOOK...	
	richard@sansswellsodas.onmicr...	HoldViewed	ComplianceAudit\ComplianceH...	

Figure 7: Unified Audit Log Review

By enabling these advanced logging settings, SANS Swell Soda Inc.'s Microsoft Office 365 gained critical visibility into adversary activity and simplified the time and difficulty involved in administrative log reviews.

Mitigation 2: Policy Templates

Another valuable tool in an Office 365 E5 tenant administrator's toolbox is Microsoft's included Data Loss Prevention (DLP) suite. While the capability's applicability to intellectual property is large enough to form its own separate analysis, one fundamental building block of DLP, the policy template, can be quickly implemented

and used by administrators to gain visibility into key intellectual property as a logging mechanism.

Office 365 and Exchange Online include several pre-built content searches (called Policy Templates) to be utilized through the Compliance and Trust Center to track and prevent unintended disclosures of sensitive information. By integrating these templates with native Office 365 transport functionality, Microsoft enables administrators to both track and analyze the movement of information covered by the content policy. At a tenet level, the policy decides if the movement should be allowed, should present a warning to the sending user, or should be prevented entirely. Over 90% of the included templates relate to the active defense of fiscal or international regulatory compliance (such as PCI policy templates preventing emails containing over four potential credit card numbers from being emailed). Still, custom templates can be created within minutes to apply in an audit-only configuration to track sensitive content. The allowance of the custom policy's disposition to “alert” without actively interfering with the transfers (and potentially introducing false positive work stoppages) presents small- and medium-sized businesses a built-in potential early warning sensor of an intrusion as the attacker both searches for and attempts to exfiltrate the data.

To apply this countermeasure to the SANS Swell Soda Inc. analysis tenet, a basic custom Policy Template was developed (Figure 8). The template's goal was to detect the movement of data that contained keyword ingredients in the Secret Recipe (Caramel Soda, Citric Acid, and SANS Soda Extract), and if these contents were discovered, to raise an event and send an email to the tenet administrator. The template was created and emplaced in three minutes and was deployed to the tenet and began acting in less than twenty minutes.

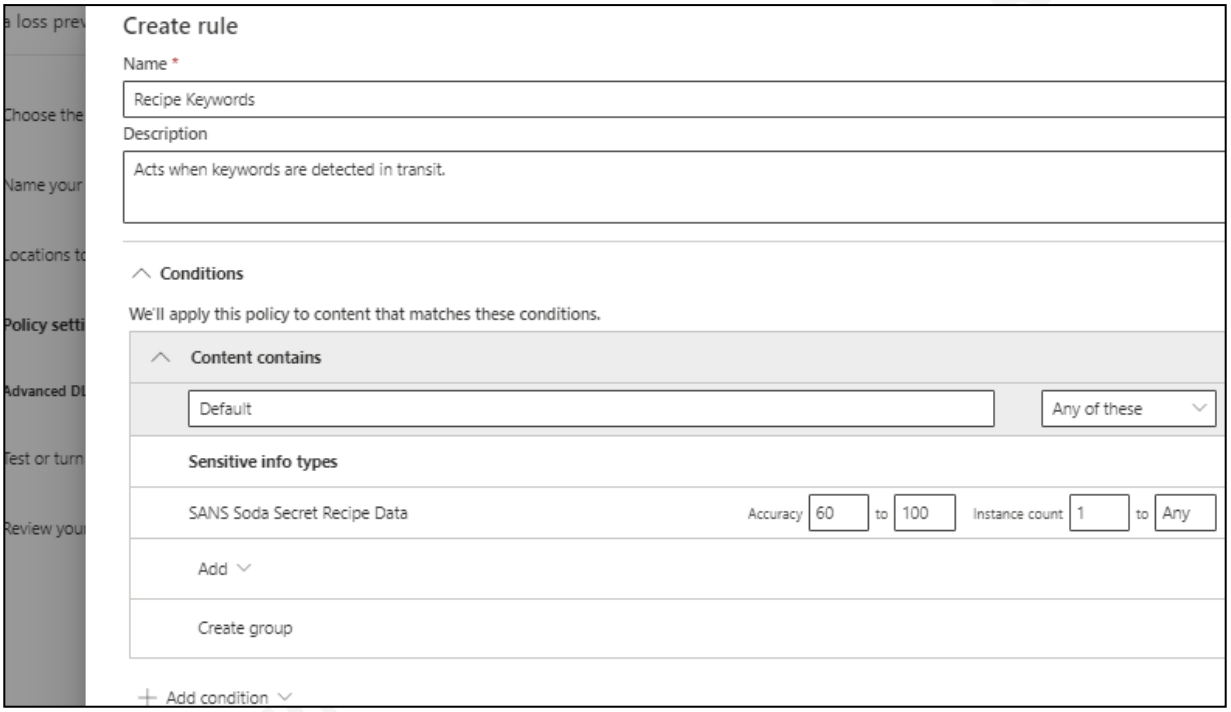


Figure 8: SANS Swell Soda DLP Policy Template for Secret Ingredients

After the template was installed, search results from the Advanced eDiscovery case were exported to the SANS Swell Soda's Azure Storage blob. While the export was still successful (the template's policy was only designed to alert), an email was also instantly dispatched to the Global Administrator alerting to both the source and destination of the exfiltration, the content being shipped, and the names of the file that was attached to the email containing the template's keywords. Several logging artifacts were also entered into the Unified Log interface highlighted in the Advanced Logging section. When combined with the extended retention policy created, SANS Swell Sodas would have an almost complete attack timeline even if the live alert was missed.

Mitigation 2 Key Observations

The simplicity of installation and high-level organizational visibility gained by installing a Policy Template makes it a force multiplier, especially in small- to medium-sized businesses who may lack dedicated resources and knowledge on advanced Office 365 compliance and auditing features. Additionally, with the ability to avoid false

positives actually impacting the business's workflow, Policy Templates provide a rare intrusion detection system in a cloud environment that is included as part of the E5 tenet.

3.2. Attacking SANS Swell Sodas, Inc. – Improved Defenses

The two living off the land defensive countermeasures analyzed in Section 3.1 were applied in a combined manner to the SANS Swell Sodas E5 tenet before the initial set of tactics from Section 2 were re-executed. Tests were again conducted on a different day of the week to minimize log contamination from previous observations, and only the Unified Log was viewed to attempt to identify the presence of the attacker and the tactics in use. Figure 9 presents the same view of the artifacts from Section 3 with the potential detection controls applied.

Tactic	Artifacts Created	Accessibility of Artifacts	Likelihood of Detection
Litigation Hold	49	2	2
Advanced eDiscovery	15	1	1

Figure 9: Detection Success Matrix in Enhanced Configuration

The countermeasures implemented had a drastic impact on the Global Administrator and business' ability to detect these attack tactics by producing clear and concise logs that detailed exact actions taken by the adversary on their targets and greatly increased the ability to either instantly respond to the tactics being utilized. These controls required little additional knowledge or time commitment by the implementing organization and additionally had no potential to cause business interruption as the controls were enacted.

4. Conclusion and Future Implications

By implementing two native countermeasures that increased visibility into administrator and employee actions in an Exchange Online hosted environment in Microsoft Office 365, both quantifiable and qualifiable impact was demonstrated in a small- to medium-sized business' ability to track an adversary using living off the land tactics in a compromised organization. These countermeasures came at no additional

licensing cost to the implementing business as both were included in the current license tier already being paid for, and both required little time investment from administrators who did not monitor the Exchange tenet at all times. These critical countermeasures were:

- Enabling Advanced Logging tenet-wide and reviewing Unified Logs
- Creating basic Data Loss Templates to monitor data movement

During the course of this research, multiple opportunities for improving the detection methodologies outlined here to allow them to be applied in a more active nature were observed. While this may not be feasible for limited-resourced businesses, the use of Office 365 native Compliance Features to defend organizations against adversaries using living off the land cloud-tactics is a worthwhile investment of research efforts and documentation work to enable defense of the larger community. Additionally, mapping both offensive and defensive tactics to community standards such as MITRE's ATT&CK Framework and the CIS Critical Cloud Security Controls framework as part of an ongoing continuous monitoring program will even more efficiently allow defenders to prepare for this increasing attack opportunity.

Small- and medium-sized businesses continue to increase the potential for compromise of their most critical and sensitive communications systems by migrating them to cloud instances. By applying the techniques outlined by this research and continuing to stay informed on adversary tactics, they can shrink their attack surface and become better postured to fend off modern threats operating in these environments.

Rebel Powell, rebelpowell@gmail.com

5. References

BitGlass Inc. (2019, November 5). 2019 BitGlass Cloud Adoption Report - A is for Adoption. A Is for Adoption. https://pages.bitglass.com/rs/418-ZAL-815/images/Bitglass_AforAdoption.pdf

Coles, C., 2016. Office 365 Adoption Rate, Stats, And Usage. [online] Available at: <https://www.skyhighnetworks.com/cloud-security-blog/7-charts-reveal-the-meteoric-rise-of-office-365/> [Accessed 21 May 2020].

Coreview, 2020. Office 365 License Optimization Report - Coreview. [online] CoreView. Available at: <https://www.coreview.com/resources/whitepaper/microsoft-office-365-license-optimization-report/> [Accessed 21 May 2020].

Crowdstrike Inc. "2019 CrowdStrike Global Threat Report." Crowdstrike.com, April 13. 2020, www.crowdstrike.com/resources/reports/2019-crowdstrike-global-threat-report/.

Department of Homeland Security (CISA), 2019. Microsoft Office 365 Security Observations. [online] Us-cert.cisa.gov. Available at: <https://us-cert.cisa.gov/ncas/analysis-reports/AR19-133A> [Accessed 26 May 2020].

Faou, M., 2019. [online] TURLA LIGHTNEURON One email away from remote code execution. Available at: <https://www.welivesecurity.com/wp-content/uploads/2019/05/ESET-LightNeuron.pdf> [Accessed 19 May 2020].

Faraglia, D. (2020). Faker (Version 4.11) [Computer software]. Retrieved April/May, 2020, from https://github.com/joke2k/faker

FBI iC3, 2016. 2016 Internet Crime Report. [online] Internet Crime Complaint Center. Available at: <https://pdf.ic3.gov/2016_IC3Report.pdf> [Accessed 21 April 2020].

Fraizer, J. and Zohlen, C., 2017. 5 Ways Legal And Compliance Teams Can Benefit From Office 365 Migration | Corporate Counsel. [online] Corporate Counsel. Available at: <https://www.law.com/corpcounsel/almID/1202792943627/5-Ways-Legal-and-Compliance-Teams-Can-Benefit-from-Office-365-Migration/> [Accessed 25 April 2020].

Halfin, D., 2020. Search For Ediscovery Activities In The Audit Log - Microsoft 365 Compliance. [online] Microsoft Technet. Available at: <https://docs.microsoft.com/en-us/microsoft-365/compliance/search-for-ediscovery-activities-in-the-audit-log?view=o365-worldwide> [Accessed 5 May 2020].

Leydon, J. (2020, March 13). Interview – Corelight's Richard Bejtlich on cyber warfare and the origin of the term 'APT'. The Daily Swig . Retrieved May 5, 2020, from https://portswigger.net/daily-swig/interview-corelights-richard-bejtlich-on-cyber-warfare-and-the-origin-of-the-term-apt

LogicWorks, 2020. 2020 Survey Report: Challenges In AWS Transformation. [online] 2020 Survey Report. Available at: <https://go.logicworks.com/2020-cloud-transformation-challenges> [Accessed 19 May 2020].

Mandiant, 2018. Mandiant MTRENDS 2018. [online] FireEye.com. Available at: <https://investors.fireeye.com/static-files/b7dcb16f-44a8-4cfb-927f-efeed397dd52> [Accessed 19 May 2020].

Rebel Powell, rebelpowell@gmail.com

Microsoft Inc, 2019. Office 365 meets evolving eDiscovery challenges in a cloud-first world. [online] Microsoft.com. Available at: <https://www.microsoft.com/en-us/itshowcase/office-365-meets-evolving-ediscovery-challenges-in-a-cloud-first-world> [Accessed 5 May 2020].

MITRE, 2020. Email Collection, Technique T1114 - Enterprise | MITRE ATT&CK®. [online] MITRE ATT&CK Office 365. Available at: <https://attack.mitre.org/techniques/T1114/> [Accessed 21 May 2020].

Proofpoint Inc, 2015. Proofpoint's Role In Office 365 Security. [online] Available at: <https://www.proofpoint.com/sites/default/files/PROOFPOINT%20FOR%20OFFICE%20365-ROLE-IT-SECURITY.pdf> [Accessed 18 April 2020].

The RadiCati Group, Inc., 2020. Email Statistics Report, 2020-2024. [online] Radicati.com. Available at: <https://www.radicati.com/wp/wp-content/uploads/2020/01/Email_Statistics_Report,_2020-2024_Executive_Summary.pdf> [Accessed 13 April 2020].

SANS Institute and Microsoft Inc., 2019. Bye Bye Passwords: New Ways To Authenticate. [online] Query.prod.cms.rt.microsoft.com. Available at: <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE3y9UJ> [Accessed 21 April 2020].

Appendix
Logs Enabled by Full Auditing

```
PS C:\Windows\system32> Get-Mailbox -Identity richard@sansswellsodas.onmicrosoft.com | select *audit*


AuditEnabled     : True
AuditLogAgeLimit : 90.00:00:00
AuditAdmin       : {Update, MoveToDeletedItems, SoftDelete, HardDelete...}
AuditDelegate    : {Update, MoveToDeletedItems, SoftDelete, HardDelete...}
AuditOwner       : {Update, MoveToDeletedItems, SoftDelete, HardDelete...}
DefaultAuditSet  : {Admin, Delegate, Owner}



PS C:\Windows\system32> Get-Mailbox -Identity richard@sansswellsodas.onmicrosoft.com | select-object -expandproperty AuditOwner
Update
MoveToDeletedItems
SoftDelete
HardDelete
UpdateFolderPermissions
UpdateInboxRules
UpdateCalendarDelegation
MailItemsAccessed
```

Last Updated: October 26th, 2020

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS Sydney 2020	**Sydney, AU**	**Nov 02, 2020 - Nov 14, 2020**	**Live Event**
SANS Secure Thailand	**Bangkok, TH**	**Nov 09, 2020 - Nov 14, 2020**	**Live Event**
APAC ICS Summit & Training 2020	**Singapore, SG**	**Nov 13, 2020 - Nov 28, 2020**	**Live Event**
SANS Community CTF	**,**	**Nov 19, 2020 - Nov 20, 2020**	**Self Paced**
SANS Local: Oslo November 2020	**Oslo, NO**	**Nov 23, 2020 - Nov 28, 2020**	**Live Event**
SANS OnDemand	**OnlineUS**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**