Global Threat Intelligence Center

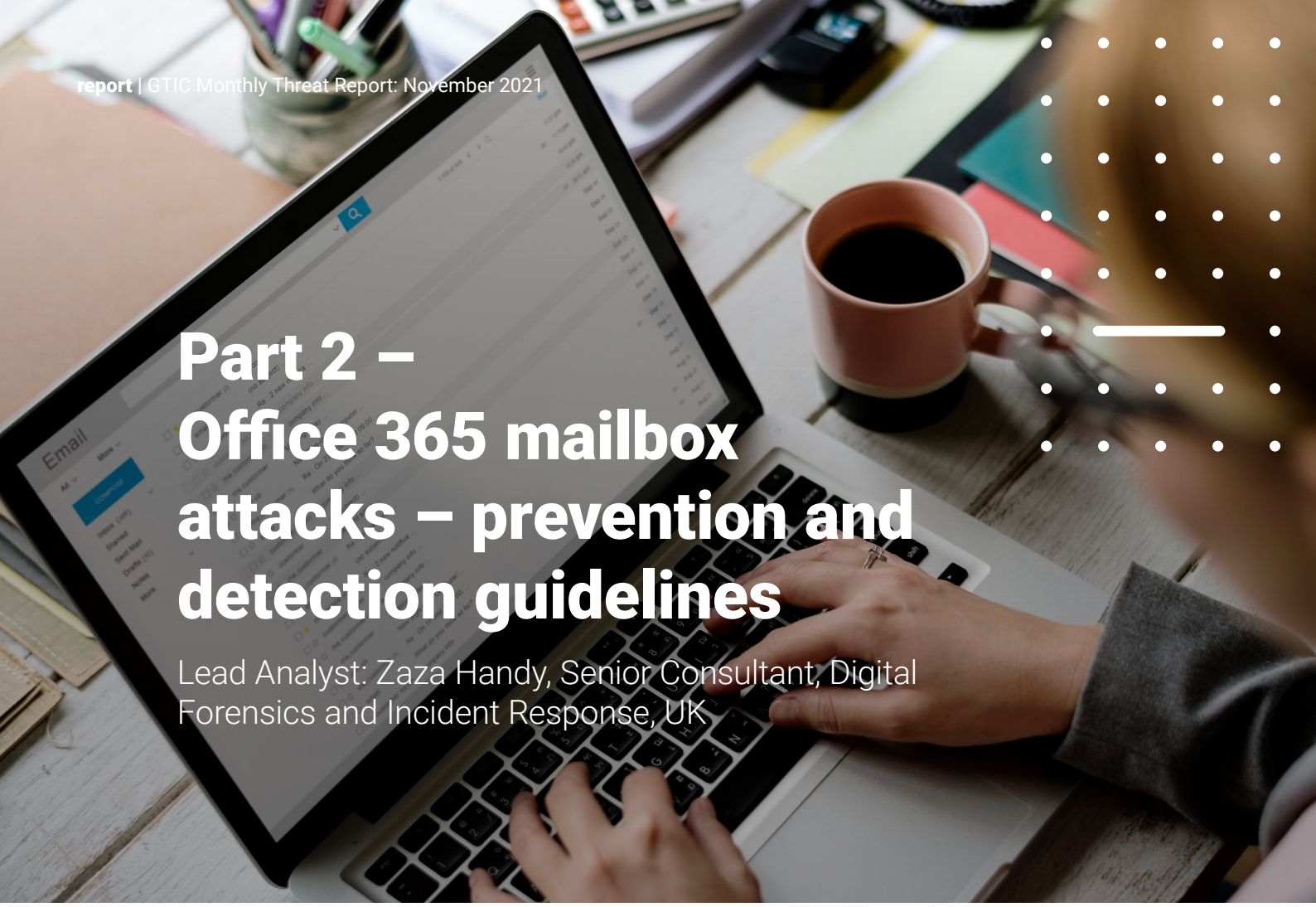
# Monthly Threat Report

November 2021

## Contents





# Part 2 – Office 365 mailbox attacks – prevention and detection guidelines

Lead Analyst: Zaza Handy, Senior Consultant, Digital Forensics and Incident Response, UK

**This article is part two of a discussion on attacks targeting Office 365 mailboxes and focuses on guidance to prevent and detect attacks. The first part of this article, included in our October Monthly Threat Report, covered how and why such attacks occur.**

Identification of Mailbox attacks is not without challenges. Remote working with inadequate controls can limit the visibility organizations have into DNS and web activity.

One of the first steps in understanding how to detect and prevent such attacks is by improving your understanding of actions an attacker may take beyond simply capturing mailbox credentials.

## Post compromise actions

### Additional reconnaissance

A successful attacker will perform additional reconnaissance, including identifying contacts, shared access rights, and the victim's role in the company if not previously known.

Attackers also dump the mailbox, read and search it on their local machine. Attackers can perform this via both automated and manual techniques.

### Performing phishing against new stolen contacts

If the first mailbox does not have the value for which the attacker is looking, they continue harvesting contact details from that mailbox and repeat the process, targeting additional users.

### e-discovery

Attackers often run an e-discovery tool on the mailbox to search for specific keywords. Nigeria-based actors are notorious for Office 365 compromises that target a business's finance data. They would search entire mailboxes for keywords such as invoice, account number, sort code, debit card, credit card, payment or similar phrases associated with valuable information and use that information to help identify and target additional users and internal systems.

### Send emails

Attackers regularly send targeted emails to coworkers, partners and customers, masquerading as the user. We commonly observe that the attackers send emails from the existing account with the Reply-To field reset to the attacker's account. Replying to the email from the compromised account initiates communication with the attacker outside of the corporate environment.

The email header in Figure 1 is from an email that was a response from the victim company's partner to an email sent from a compromised mailbox. The Reply-To email is not the domain of the original sender. The attacker is delivered a copy of the email to his @dr.com address shown in the Reply-To line.

**From:** <businessmail@compromisedorg.co.uk>
**To:** Accounts Receivable Team <AccountsReceivable@PartnerVictimDomain.com>
**Subject: RE:** Payment from TargetedPartnerOrganization for Over Payment ON Claims
**Reply-To:** "businessmail@compromisedorg.co.uk"
<businessmail-compromisedorg.co.uk@dr.com>
**X-ASG-Orig-Subj:** RE: Payment from TargetedPartnerOrganization for Over Payment ON Claims
**User-Agent:** Roundcube Webmail/1.4.11
**Message-ID:**<0dcbeafcda007234e40feec3d6d59f96@compromisedorg.co.uk>
**X-Sender:** businessmail@compromisedorg.co.uk

*Figure 1: Email header showing attacker ability to receive all replied emails sent to unsuspecting senders.*

At this stage, it takes the vigilance of paranoid employees to stall the progression of the fraud. The person at the targeted partner organization would need to recognize that the Reply-To address is not the proper domain to stop the fraudulent activity.

## Prevention

### Security awareness and training

Effective security awareness and training is a fundamental step in defeating phishing attacks, and thus, in preventing mailbox attacks before they happen. Organizations must train users in security measures and habits in context of their jobs.

### Block spam and malicious email

Spam filters can help prevent phishing emails before attackers can harvest credentials. Organizations can also configure email filters to reduce other potentially hostile emails and prevent email spoofing.

## Detection

### Detect attempts to harvest credentials

Organizations can continuously review web traffic data to help identify successful connections to suspicious sites and identify potentially compromised accounts.

### Audit mailbox and unified logs

Organizations should continuously review mailbox audit logs to hunt for anomalies. Figure 2 shows detail from one user mailbox accessed multiple times within a brief period from multiple client IP addresses. This shows that attackers had used a wide variety of endpoints to access the mailbox, which would indicate likely compromise.

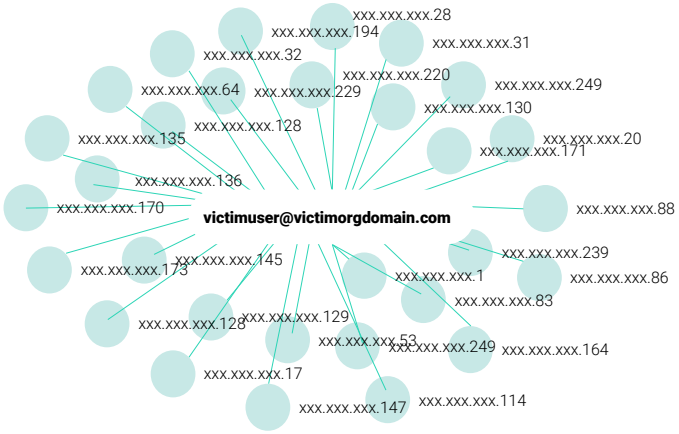



*Figure 2: Multiple mailbox access from different Client IPs*

Similarly, these logs can identify accounts with anomalous failed login activities and accounts that show unusual login activity from multiple locations. As shown in Figure 3, an email account with numerous failed logins from multiple locations is even more suspicious than simple access from multiple locations.

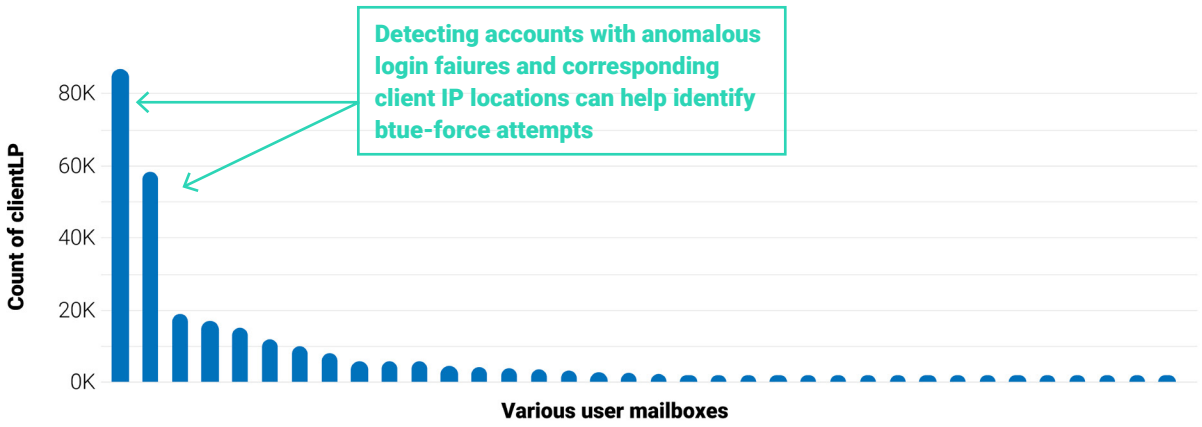



*Figure 3: Mailbox audit showing abnormal mailbox activity for victim mailbox*

### Constantly review mail forwarding rules

An attacker who has successfully compromised an exchange online account will often create rules to forward copies of all sent emails. Review and reconcile all mail forwarding rules on Office 365. This will help to remediate an attacker's actions and serves as routine threat detection.

Organizations can also **configure email filters to reduce other potentially hostile emails** and prevent email spoofing.

### Review MailItemsAccessed audit records

Organizations usually audit MailItemsAccessed records post-compromise to identify messages accessed by an attacker. Organizations can run this same audit to check sensitive accounts for potentially unauthorized access. Microsoft has provided extensive information on forensics of mailbox access, including where email was read from bind, and if a client was used to sync the mailbox (Sync activity). Please see more details at **Use Advanced Audit to investigate compromised accounts - Microsoft 365 Compliance | Microsoft Docs**. Microsoft has also provided PowerShell scripts for mailbox and unified mailbox access audit logs.

Organizations will need an Office 365 E5 license to leverage forensics capability and audit MailItemsAccessed records.

## Additional preventive recommendations

### Implement multi-factor authentication

Enabling multi-factor authentication on internet-facing services such as email is a strong preventive control. Organizations should also extend multi-factor authentication to other services such as VPN access.

### Block the indicators of compromise

Once the organization can identify attacker IPs or known malicious IP addresses, block the IP addresses and search for other attack victims.

### Review password policy

A strong password policy is important, but becomes crucial when authentication is only single-factor. If the password renewal period is 90 days, an attacker can potentially access the business data via compromised accounts for the entire time remaining in that period.

### Educate users

During our incident investigations, more than one user retrieved and acted on a phishing mail that had been quarantined. Continuous training on identifying social engineering tactics arm users with the ability to better recognize initial phishing attacks and fraudulent emails.

### Review and remediate attack

Once the organization has detected compromise, review and remediate all compromised accounts. Organizations should report any breach to the appropriate legislation, law enforcement, and compliance bodies and consider sharing indicators of compromise (IOCs) with the community.

## Summary

Unfortunately, email compromises are not especially difficult for a dedicated attacker. On top of that, a comprehensive solution to prevent, detect, and recover from an email compromise can be complex. But, given how much attackers are currently targeting such accounts, organizations should consider what practical measures can improve their ability to manage such compromises.

**A strong password policy is important**, but becomes crucial when authentication is only single-factor.

Spotlight

# Upcoming shift in the approach to securing OT

Lead Analyst, Zhanwei Chan, Global OT/IoT Practice Lead, Australia

**Over the last few years, OT teams have been driving most requirements to secure Operational Technology (OT) and Industrial Control Systems (ICS). The OT team has understood the need to continue to innovate – securely. An interruption caused by malware, or any other threat, can be very costly.**

**OT teams who had not been exposed to modern cybersecurity risks often drove the early days of those conversations. To be successful, we needed to prove to OT stakeholders that there are cybersecurity risks in the OT network.**

## What is happening

In more recent months, there has been a shift in process and approach. The existing cybersecurity team and the wider IT team are getting more involved with OT implementations and management. In some cases, cybersecurity in OT/ICS networks is now the responsibility of the existing IT team. The primary conversation owner has moved from the OT team to the IT team.

Historically, the OT team is might not even included in initial discussions. IT's cybersecurity team has typically kicked off cybersecurity initiatives for OT/IoT networks.

## Why it is happening

The shift of cybersecurity control from OT to IT was inevitable for many reasons:

- In many cases, network infrastructure in the OT environment (e.g., Switch, VLAN, physical cabling, and even IP addressing) has been managed by IT. Cybersecurity for OT was just a natural addition to the portfolio and responsibility of the IT team.
- Existing technical skills and support in IT. The technology used to secure OT networks is not exactly new to cybersecurity. The IT team better knows vendor and maintenance skills since they have supported operational environments for years. It is often more practical to use existing skills within the organization than to hire and manage new staff within the OT team.
- The OT team needs to focus on engineering to meet production requirements. The IT organization is more prepared to plan and support the infrastructure required by the OT team.
- OT is using more IT-related equipment – especially for analytics. There have also been many massive projects to migrate OT Data Center into a data center shared with IT.

## What it means

We do expect this IT/OT convergence trend to continue. As a result, it will have two main effects:

- Cybersecurity for OT will be more aligned with IT. Specific limitations and requirements for the OT network will continue to exist. However, OT-related cybersecurity will continue to evolve.
- There will be greater pressure on IT and OT teams to work together more. Specifically, the IT team will need to understand the OT network better. At the same time, the OT team will need to include IT-related processes and controls, such as in review and evaluation processes.

## How to prepare

We have seen massive evolutions in cybersecurity: Endpoint security is critical, and cloud adoption is accelerating. The convergence of IT/OT should not be too surprising. There are some areas organizations can prepare for:

- **Connectivity of OT network to IT and internet.** OT networks have traditionally been isolated from each other. However, there's an increasing demand for OT networks to be connected to IT and external networks.
- **Demand for Remote Access.** We've already seen the explosion of remote support because of COVID-19. Many IT teams and organizations are supporting remote working. If IT and OT are converging, how will remote work and remote support be adapted for OT?
- **Increased rate of change.** Changes in the OT network tend to happen rarely, and are usually predictable. However, with Industry 4.0 and 5.0, will change be more frequent and required? For example, what kind of requirements will there be for more frequent cybersecurity patching or network changes to accommodate engineers who work onsite once a month.
- **Continued evolution of IT technology.** How would OT networks use and adopt machine learning, super-fast 5G network, cloud-delivered services, and ever-growing cybersecurity requirements associated with these evolutions in technology?

The existing **cybersecurity team and the wider IT team are getting more involved** with OT implementations and management.

## What can the IT team do to secure OT today?

The trend that we have observed lately indicates more support is required to secure OT networks. This includes OT teams recognizing the need for security, IT teams recognizing the need to collaborate, and management recognizing the need to prioritize collaboration and security. Best of all, OT teams want to work with IT. The first steps should always be:

- Both management and IT need to understand that the OT network has limitations. The majority of IT-based technology will not be suitable to secure OT. To properly secure OT, we need new cybersecurity solutions to bridge the requirements between OT and IT environments.
- IT needs to be conscious that the OT team will continue to own the OT network and processes. OT understands the operational environment and constraints, which are different than those of IT. The OT team's core responsibility is to ensure the organization is producing output. IT and OT must build a relationship with co-operation and empathy.
- The OT team will need cybersecurity assistance. However, OT teams tend to be cautious when making changes. It will be necessary for IT and OT to build a collaborative working environment based on trust.

Spotlight

# Tokyo 2020 cybersecurity – going for gold

Lead Analyst: Mihoko Matsubara, CISSP, Chief Cybersecurity Strategist, NTT Corporation, Japan

**Japan successfully completed the Tokyo 2020 Olympic and Paralympic Games on 5 September without any significant disruption to the operations by cyberattacks during the event. The Olympics were not completely free from cyber threats, but hostile activity appeared as mostly minor cybercrime attempts. For example, cybercriminals created multiple phishing websites claiming to broadcast the torch relay and Olympic Games opening ceremony, attempting to steal victims' personal and credit card information. Fortunately, sources have reported no damage as of today.**

Tokyo 2020 stakeholders had anticipated cyber attacks to achieve financial gains, damage Japan's reputation and trust, or disrupt the operations of Tokyo 2020. Japanese Supply Chain Cybersecurity Consortium (SC3) Chairperson Nobuhiro Endo issued an open letter in July 2020. In the letter, he urged member companies and their business executives to ensure cyber defenses were implemented to protect Tokyo 2020 and Japan from cyber espionage, disruptive cyberattacks such as distributed denial of service (DDoS), ransomware, and cybercrimes for money and personal information. The consortium brought together small and large companies, as well as trade associations, to enhance Japan's cybersecurity and supply chain risk management.

Dr. Brian Gant, Assistant Professor of Cybersecurity at Maryville University, praised Tokyo 2020's cybersecurity as 'a real success story' in his Security Magazine article dated 17 August, attributing the success to their 'aggressive preemptive measures.' Olympic Minister Tamayo Marukawa explained during a press conference on 14 September that close public-private partnerships achieved the safe and secure Tokyo 2020, adding that stakeholders conducted practical cyber exercises that proved very helpful. The Japanese government ran the Security Coordination Center to share information on cyberattacks, natural disasters, and terrorism between the government, the Tokyo 2020 Organising Committee, and other stakeholders.

Tokyo 2020 also showcased different technologies for digital transformation and security. Intel provided a light show with 1,825 drones above the Olympic Stadium on the day of the 2020 Summer Olympics opening ceremony in July. ALSOK, a security service firm based in Tokyo, offered drones and security robots with artificial intelligence-driven image recognition technology to secure Tokyo 2020. NEC Corporation contributed a facial recognition system to scan people who entered Tokyo 2020 stadiums. This was the first time in the history of the Olympics and Paralympics that the Games used facial recognition technology.

Japan won a gold medal for cybersecurity. The country needs to compile lessons learned and share them with Paris 2024, Los Angeles 2028, and other major international events. Olympic and Paralympic Games are a complex global event. Working with 190 countries, many sports associations, local government at the central and municipal level, sponsors, and critical infrastructure companies was a tremendous and successful enterprise. Japan's expertise in digital transformation, cybersecurity, and international coordination is proven gold, and those experiences are now in high demand.

## NTT's Global Threat Intelligence Center

The NTT Global Threat Intelligence Center (GTIC) protects, informs, and educates NTT Group clients through the following activities:

- threat research
- vulnerability research
- intelligence fusion and analytics
- communication to NTT Group clients

The GTIC goes above and beyond the traditional pure research organization, by taking their threat and vulnerability research and combining it with their detective technologies development to produce applied threat intelligence. The GTIC's mission is to protect clients by providing advanced threat research and security intelligence to enable NTT to prevent, detect and respond to cyberthreats.

Leveraging intelligence capabilities and resources from around the world, NTT's threat research is focused on gaining understanding and insight into the various threat actors, exploit tools and malware – and the techniques, tactics and procedures (TTP) used by attackers.

Vulnerability research pre-emptively uncovers zero-day vulnerabilities that are likely to become the newest attack vector, while maintaining a deep understanding of published vulnerabilities.

With this knowledge, NTT's security monitoring services can more accurately identify malicious activity that is 'on-target' to NTT Group clients' infrastructure.

Intelligence fusion and analytics is where it all comes together. The GTIC continually monitors the global threat landscape for new and emerging threats using our global internet infrastructure, clouds and data centers along with third-party intelligence feeds; and works to understand, analyse, curate and enrich those threats using advanced analysis techniques and proprietary tools; and publishes and curates them using the Global Threat Intelligence Platform (GTIP) for the benefit of NTT Group clients.

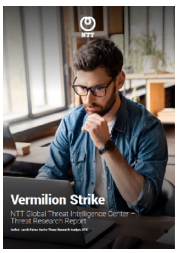
Our **Global Threat Intelligence Center** goes beyond a traditional research-only approach by combining focused research with detective technologies. This results in **true applied threat intelligence** to protect our clients with effective tools and services which reduce security risks and threats.

## Recent assets


### 2021 Global Threat Intelligence Report

Our 2021 Global Threat Intelligence Report (GTIR) is the culmination of the data the Global Threat Intelligence Center gathered and analyzed throughout the year. We produce this report by collecting a broad set of global data (log, event, attack, incident and vulnerability) to identify key cybersecurity trends of which businesses need to be aware.

**Download report**




### Vermilion Strike Report

During our threat research the GTIC used information from a public blog to initiate a deeper dive into Vermilion Strike. Vermilion Strike is a Linux reimplementation of the Cobalt Strike Beacon, built from the ground up by threat actors.

**Download report**

If you haven't already, **register to receive the Monthly Threat Reports** directly to your inbox each month. Sign up for our **Emerging Threat Advisory** and security bulletins for visibility of emerging threats and vulnerabilities that are being actively exploited across the world, sourced from our global threat intelligence platforms.


NTT