Global Threat Intelligence Center

Monthly Threat Report

October 2021

Contents

Part 1

Office 365 mailbox attacks: why and how?

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

This article is part one of a two-part story on attacks targeting Office 365 mailboxes. This article focuses on why and how the attacks happen. Part two will be included in the November Monthly Threat Report and cover how to prevent and detect such attacks.

Most organizations are surprised when they discover the type of data stored in their business email mailboxes: HR information, sensitive client data, payment card data, business trade secrets, passwords and even juicy gossip that could embarrass people or expose them to blackmail.

As organizations have embraced cloud-based services such as online Exchange mailboxes, attackers, in parallel, have been quick to recognize the opportunity.

If your organization hasn't enabled multifactor authentication for online Exchange users, you may be vulnerable to rogue mailbox access, information theft and fraudulent activity against your business, customers and trusted partners.

When we hear of an 'attack', the first thing that comes to mind is often malware. However, malware is only one tool attackers use to facilitate their activities. With successful intrusion into an organization's mail system using stolen credentials, an attacker doesn't need malware to take over email accounts, steal data and impersonate your employees to commit financial fraud or other nefarious activities. Worse yet, if the attacker can use a valid password, the organization is more likely to trust their actions since they appear to act as the employee. An attacker with valid credentials won't raise the same alarms as unauthorized activity would.

Based on our observations, mail compromises happen in stages. Often, one group performs the initial compromise, and another group facilitates post-compromise activities such as mail monitoring, financial fraud and data exfiltration. In some situations, an initial actor may sell credential data on the dark web as a service to whoever wants to engage in the post-credential-theft activity. This acquisition and use of stolen usernames and passwords may be by another attacker who has only a 'business' relationship with the attacker who initially collected the credentials.

Initial mailbox compromise

The first step in any mailbox compromise is obtaining valid mailbox credentials – username and password. Attackers tend to use proven social engineering techniques to harvest user credentials. There have been cases where a successful brute force attack enabled an initial mailbox compromise, but most of the time, users hand over credentials on a forged Office 365 landing page hosted on an attacker-controlled website.

The more credentials an attacker can gather the better, however, the attacker doesn't need to harvest many credentials to accomplish their goal. Even a single set of valid credentials can be invaluable if they're related to the right target. For targeted attacks, attackers tend to focus on employees in the finance or executive teams.

In a case we recently investigated, attackers obtained the account credentials of a single user in finance. The compromised credentials allowed the attacker to identify the shared mailboxes to which the user had access, and created mailbox rules that further compromised data beyond the user's mailbox. This allowed the attacker access to many more emails than those of the initial user.

Below we see a typical phishing email sent to the unsuspecting user victimuser@victimorgdomain.com. The phishing lure includes a link for the user to 'Release' some held emails. This compels the user to access the attacker's credential harvesting page by selecting the 'Release Emails' button.

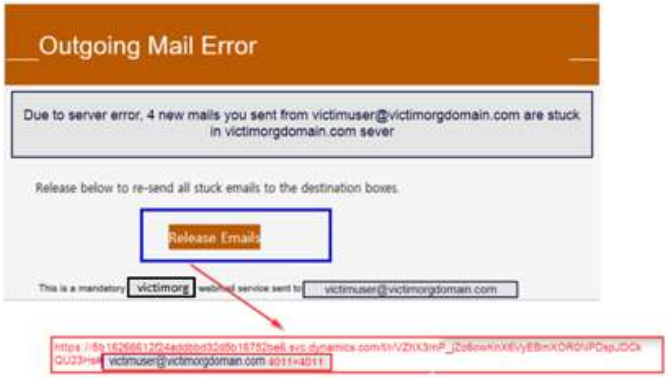


Figure 1: Example phishing email sent to the victim

If the organization recognizes the attacker's URL as suspicious, some organizations might restrict access. If the user is allowed access to the URL, the site will prompt them to enter their mailbox username and password, effectively providing their credentials to the attacker.

'The more credentials an attacker can gather the better, **however, the attacker doesn't need to harvest many credentials to accomplish their goal.'**

Zaza Handy, Senior Consultant, Digital Forensics and Incident Response, UK

Using those credentials

Attackers regularly send targeted emails to coworkers, partners and customers, masquerading as the user. We commonly observe the attacker sending 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 most common motive in most of our engagements was financial, where the attacker actively attempts to convince the receiving party to amend payment details on invoices.

The header in Figure 2 is from an email that was a response from the victim company's partner email sent from a compromised mailbox. The Reply-To email isn't 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. The goal was to transfer funds to an account to compensate for the alleged 'Over Payment.'

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 2: Email header showing attacker ability to receive all replied emails sent to unsuspecting senders.

In most cases, the emails don't include overt actions that would indicate compromise. The attacker's goal is to stay hidden while coercing employees and partners into taking fraudulent activity.

Unfortunately, at this stage, it often takes the vigilance of well-trained and security-minded employees to identify the attempted fraud. The person at the targeted partner organization would need to recognize that the "Reply-To" address isn't the proper domain to stop the activity.

For additional guidance on how to recognize, detect and prevent such mailbox attacks, please read part two in our November Monthly Threat Report. Click here to subscribe to our Monthly Threat Report series and receive a copy of next month's Report directly to your inbox.

The layered infrastructure operated by APT29

Lead Analyst: Threat Detection Team, Sweden

After public reporting of APT29 activity, analysts within NTT have mapped previously unseen layers of APT29 infrastructure. The most recent activity included targeting email servers belonging to diplomatic entities located in South America and Northern Africa. APT29 is a threat actor commonly associated with a national intelligence service and has been widely reported to conduct espionage operations.

NTT initiated this research after RiskIQ reported their own research of command and control servers of the WellMess malware, operated by APT29. We discovered that some of the reported WellMess command and control servers (C2s) are used as layer 2 (L2) operator hosts (OH), while there is also a layer 1 (L1) OH in contact with the victim's email server. The targeted email servers are running open-source webmail clients that have a history of vulnerabilities. Recent reporting by the National Cyber Security Center of the UK on APT29 activity confirms APT29 operating procedure includes exploiting recently detected software vulnerabilities (as described in Further TTPs associated with SVR cyber actors, and APT29 targets COVID-19 vaccine development).

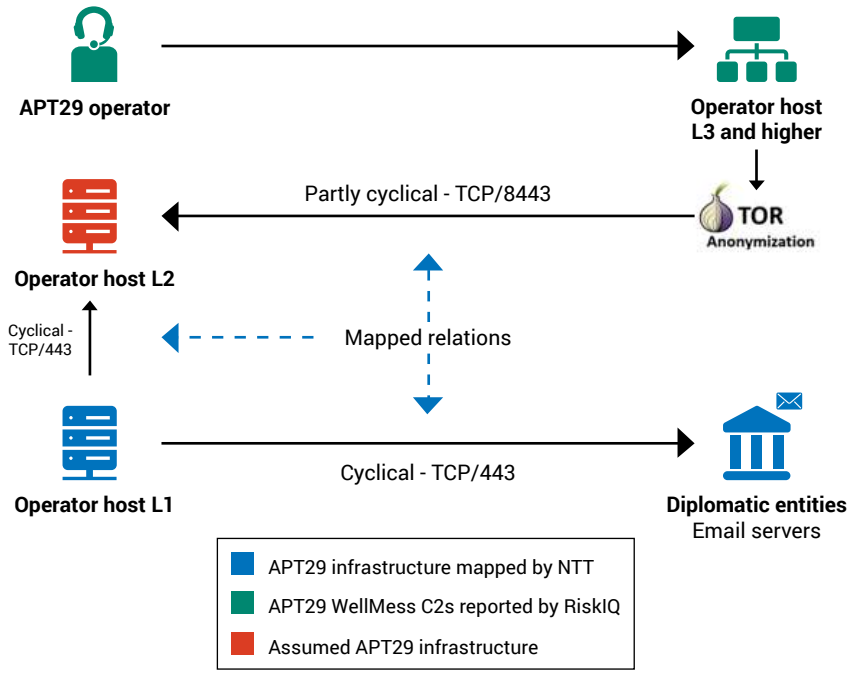


Figure 3: APT29 infrastructure

As is shown in Figure 3, communications in the infrastructure are cyclical. This indicates an automated framework that regularly communicates with, and possibly exfiltrates data from, the victim's email servers. This behavior includes what appears to be the actor, connecting to L2 OH over port TCP/8443 with anonymization through TOR at 8 PM UTC. This indicates that the actor likely included a layer 3 host in the automated infrastructure setup. The observed infrastructure setup confirms APT29's ability to perform long-term automated operations. Such infrastructure provides APT29 with the ability to continuously acquire sensitive data from the targeted environment, highlighting the espionage focus of the group.

We recommend searching for and investigate any traffic from the listed layer 1 operator hosts.

This analysis isn't meant to be a complete exploration of the APT29 infrastructure, but is representative of our ongoing analysis. The analysis performed in this report includes only a subset of the APT29 related IPs reported by RiskIQ, and the reader shouldn't necessarily assume these conclusions hold for the entire infrastructure.

How our visibility and actions help our clients

Our Threat Intelligence researchers monitor telemetry of suspicious traffic traversing our Global IP Network Service global tier-1 IPv4/IPv6 backbone network for threat indicators. Correlating such findings with the insights of our global Threat Detection (TD) and Managed Detection and Response (MDR) services enable a truly unique perspective of the evolving cybersecurity threat landscape.

Research findings on threat actors and campaigns, such as APT29, are continuously being fed from our Threat Intelligence analysts back into our services as Machine Learning capabilities, behavior models, indicators of compromise (IOCs) and Threat Intelligence. This process enhances the service's ability to efficiently monitor, detect, triage and respond to these threats on behalf of our clients, often without an initial compromise.

Indicators of compromise

Indicators of compromise where the L1 OH is sending traffic to the L2 OH on the same row:

Operator Host L1	Operator Host L1
190.97.165[.]202	141.255.164[.]40
45.114.130[.]81	111.90.151[.]120

'APT29 is a threat actor commonly associated with a national intelligence service and **has been widely reported to conduct espionage operations.'**

Threat Detection Team, Sweden

#Spotlight 2

The changing nature of ransomware

Lead Analyst: John Meyers GSIF GCIH GCFE GREM GMON GSEC GPEN, Network Associate Director, NTT DATA, US

What is the current state of the cyberthreat landscape?

Cyberthreats continue to evolve. As defenders get better at detecting and stopping attacker tactics and exploits, attackers develop new methods to gain access to targeted environments. Long gone are the days where simple security controls like antivirus could even hope to protect an organization.

The most important part of the cyberthreat landscape is understanding that both attacks and security controls continue to evolve.

How has ransomware evolved?

One of the obvious evolutions in the cyberthreat landscape has been the growth of ransomware. Ransomware threats have also become more sophisticated. Initially, ransomware was targeted at individuals to encrypt a single user device. Attackers would then demand payment of a few hundred dollars worth of gift cards. This technique was dependent on scale to be profitable. They had to encrypt lots of PCs and acquire many victims to pay to make significant money.

Next, they started targeting organizations, having realized they could extort more money from an organization than they could from an individual. Defenders responded by creating signatures to block the execution of ransomware at the initial stage of infection, but again attackers changed their tactics. They started using the same tactics as penetration teams. They would gain a foothold on a user endpoint. Then they would try to escalate their privileges or move laterally through the environment. Once they compromised a domain administrator account, attackers would use the Windows Domain infrastructure to push the ransomware to high-value servers, much like a system administrator would push an update for new software. This is the playbook of the modern ransomware gang.

Defenders countered the ransomware threat with new tactics. These tactics included better detection of ransomware. Additionally, organizations made improvements to the backup system, including versioning backup, isolated backups, and better disaster recovery planning. These tactics would allow an organization to recover from a ransomware attack without paying the ransom demand.

Attackers changed their tactics yet again and started adding the exfiltration of Intellectual Property to their tactics. They would then threaten to release information if the victim didn't pay. Today, organizations that are victims of a ransomware attack not only have their systems encrypted, but they also face the possibility of dealing with a data breach. If a victim won't pay, the attacker will publish the data on the Internet.

As discussed in our Monthly Threat Report for August 2021, ransomware has exploded over the past couple of years. We're likely facing at least a 300% growth in ransomware incidents and average payouts over the past two years. This translates into millions of detections, and something on the order of USD 20 billion in ransomware damages.

What can you do about it?

Get back to the basics.

The initial entry point for a successful attack is usually on a user endpoint system. There are a few ways to reduce the threat of this initial entry. They include patching all the software on the endpoints, limiting user privilege, network segmentation, penetration testing, and monitoring endpoints with an Endpoint Detection and Response (EDR) tool. These defense-in-depth steps can help improve the security of your environment and help reduce the threat of a ransomware attack.

Patching systems is critical to defending against modern threats to your environment. Many times, when a vendor releases a patch for software, the attackers can reverse engineer the patch to determine the vulnerability of unpatched software. They can then develop an exploit for the patched vulnerability even if one isn't publicly available. This process can take weeks, days or it can take hours. Once an attacker develops an exploit, they can use that exploit to compromise unpatched systems – either directly or by selling exploit kits or tools. Since many organizations struggle with patching software in a timely manner, the attackers often have time to compromise unpatched systems before organizations install the patch. This is especially true since some organizations may not patch effectively for years. Even worse, some vulnerabilities may not be easily patched (as they might be in firmware or have a complicated installation process).

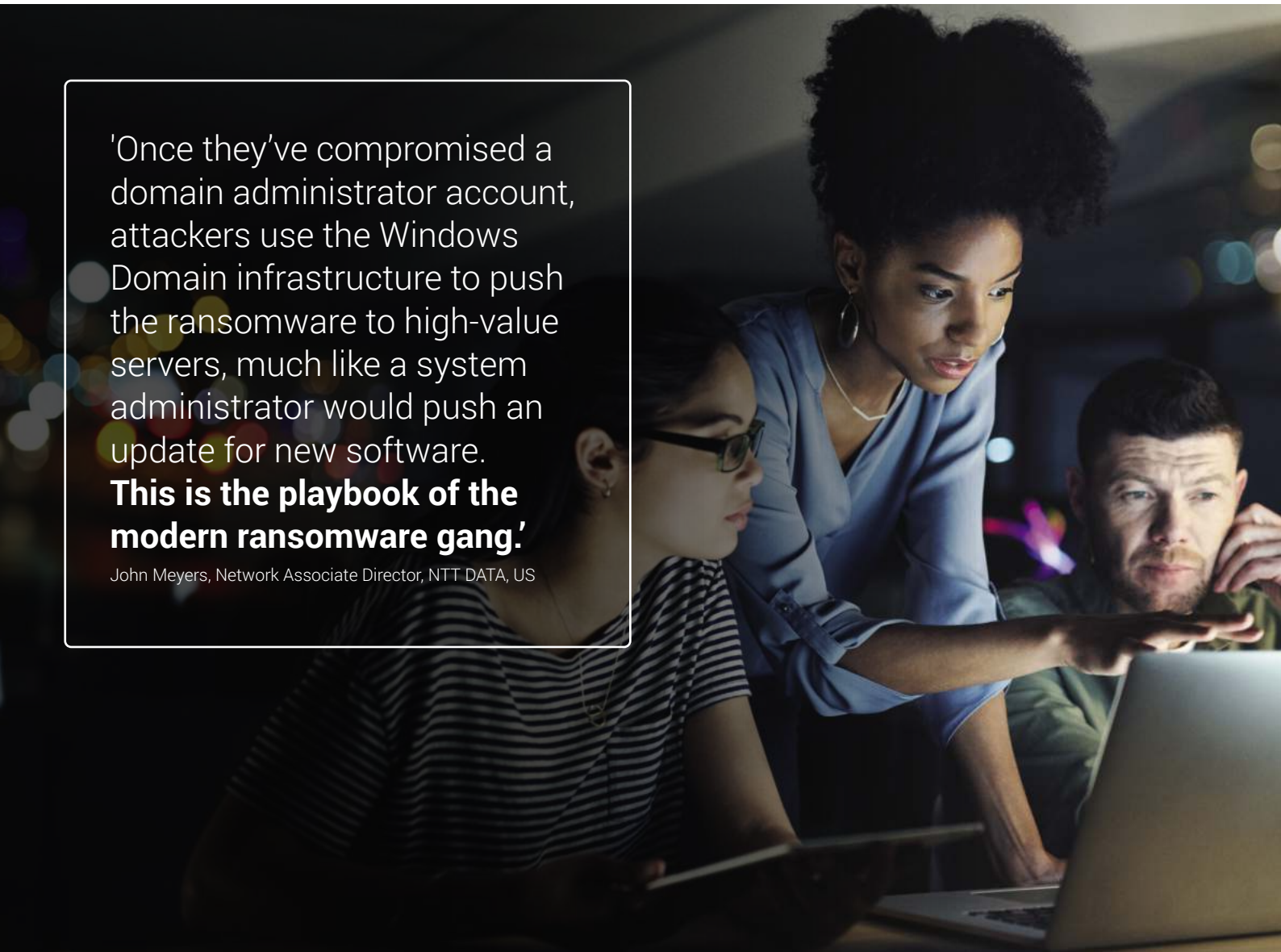
Another way to protect yourself from modern cyberthreats is to **limit user privilege on endpoints**. If your users don't have administrator privilege and can't install software, it's much harder for attackers to trick them into installing a malicious program. These malicious programs often provide the attackers with the initial access they need to further compromise the environment.

Network segmentation is another layer in the defense-in-depth approach to securing your environment. Workstations in different business units should be isolated from each other. For instance, a workstation in the HR department shouldn't be allowed to use the Remote Desktop protocol to log into a workstation in the accounting department. This can be prevented with network segmentation supported by security controls like internal firewalls and access control lists. This segmentation can also provide an additional barrier that helps detect lateral movement attackers use to compromise your environment. Adding layers of defenses in the environment will give the defenders another way to detect the attack before they reach their objectives.

Penetration testing can help you understand what an attacker will do to compromise your environment. Attacker emulation is a penetration testing technique that performs the penetration test in the same way as a specific type of attacker. You should share the results of penetration tests with your system and network operations groups so that the organization can make improvements to attacker detection. If you can isolate and identify vulnerabilities threat actors might use to attack your environment, you can also take action to eliminate those vulnerabilities from your environment and deny attackers those opportunities.

Finally, you need **visibility** into the whole environment so human analysts (threat hunters) can see what is happening in the environment. An organization can achieve visibility through improved logging configuration or an EDR tool on endpoints. Regardless of which method you use, you will need human threat hunters looking at the data. Automated alerting from tools isn't good enough to detect the sophisticated attacker. To truly understand what's happening in your environment, you need a human analyst who understands your environment by looking at the data.

In the end, there's no single solution you can put in place to eliminate all threats. But, if you can use the techniques and controls identified here, you'll have the opportunity to reduce exposure across your entire environment.



'Once they've compromised a domain administrator account, attackers use the Windows Domain infrastructure to push the ransomware to high-value servers, much like a system administrator would push an update for new software. **This is the playbook of the modern ransomware gang.'**

John Meyers, Network Associate Director, NTT DATA, US

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

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