

Water Nue Phishing Targets Execs' Office 365 Accounts

blog.trendmicro.com/trendlabs-security-intelligence/water-nue-campaign-targets-c-suites-office-365-accounts/

August 6, 2020



Cloud

A series of ongoing BEC campaigns that uses spear-phishing schemes on Office 365 accounts has been seen targeting senior positions of over 1,000 companies across US and Canada since March 2020.

By: Marshall Chen, Loseway Lu, Yorkbing Yap, Fyodor Yarochkin August 06, 2020 Read time: (words)

Content added to Folio

A series of ongoing business email compromise (BEC) campaigns that uses spear-phishing schemes on Office 365 accounts has been seen targeting business executives of over 1,000 companies across the world since March 2020. The recent campaigns target senior positions in the United States and Canada.

The fraudsters, whom we named “Water Nue,” primarily target accounts of financial executives to obtain credentials for further financial fraud. The phishing emails redirect users to fake Office 365 login pages. Once the credentials are obtained and accounts are

successfully compromised, emails containing invoice documents with tampered banking information are sent to subordinates in an attempt to siphon money through fund transfer requests.

Tracking Water Nue's activities

The threat actor behind this campaign is interesting for several reasons. It appears that their technical capabilities are limited despite being able to successfully target high-level employees globally. While their phishing tools are basic (i.e., no backdoors, trojans, and other malware), they made use of public cloud services to conduct their operations. The use of cloud services allowed them to obfuscate their operations by hosting infrastructures in the services themselves, making their activities tougher to spot for forensics. This tactic has become more commonplace among cybercriminals.

We first noticed the campaign from a large group of email domains used in phishing attempts. We found that most of the recipients hold high corporate positions, particularly in the finance department. In one of the first cases we encountered, the senior financial officer of a bank located in Africa purportedly sent a PDF invoice to a colleague, specifying a bank account in Hong Kong. The email was sent from an IP address recorded on one of the phishing sites that the attacker tested its functionality on.

The campaign is ongoing, with the threat actor switching to new infrastructures when used domain names get reported or blacklisted in systems.

Water Nue Campaign Analysis

The attackers use cloud-based email distribution services like SendGrid to deliver emails with a clickable link that redirects targets to a fake Office 365 page. (We have reached out to SendGrid and shared our findings with them.) When the target user attempts to log in, credentials are recorded through a simple PHP script.

 Water Nue attack scenario Figure 1. Water Nue attack scenario

 Sample of recorded credentials Figure 2. Sample of recorded credentials

While the techniques aren't new, the attack attempts appear to be successful, collecting over 800 credentials from company executives at the time of writing.

How accounts are targeted for phishing attacks

In a July email sent to a C-level executive, we learned that the base domain URL is U10450540[.]ct[.]sendgrid[.]net, with the final URL being *getting-panes[.]sfo2*.


 Email header "from" field shows New York and various email accounts indicating "Swiftme@{company domain names}"


Figure 3. Email header "from" field shows New York and various email accounts indicating "Swiftme@{company domain names}"

“Swiftme” appears in the phishing email headers and is accompanied by account names with forged company email domains. The displayed email header “from” and subject also pretend as a voicemail service. “Swiftme” is possibly a nod to electronic or wire transfers and reveals the campaign’s purpose after harvesting credentials.


 Email sample Figure 4. Email sample

It should be noted that the SendGrid platform does not appear to attach the X-Mailers originally. Emails with different X-Mailers and headers are likely appended through tools that can confuse scan engines. Here are some of the X-Mailers we observed:

- | **X-Mailer:** Mozilla/5.0 (Windows; U; Win98; de-AT; rv
- X-Mailer:** Claws Mail 3.7.6 (GTK+ 2.22.0; x86_64-pc-linux-gnu)
- X-Mailer:** Mozilla 4.7 [en]C-CCK-MCD NSCPCD47 (Win98; I)
- X-Mailer:** iPhone Mail (8A293)
- X-Mailer:** Opera7.22/Win32 M2 build 3221
- X-Mailer:** ZuckMail [version 1.00]
- X-Mailer:** CommuniGate Pro WebUser v5.3.2

 A phishing site imitates Office 365 login Figure 5. A phishing site imitates Office 365 login
The originating IP of Water Nue’s test/deployment machine was left in a clear text file in the phishing site’s server for collected credentials.

 Sitemap Figure 6. Sitemap

 The landing page index.html has a dummy speech functio Figure 7. The landing page index.html has a dummy speech functio




 While the main collection function resides in app.js, command and control (C&C) location is embedded in JavaScript code


Figure 8. While the main collection function resides in app.js, command and control (C&C) location is embedded in JavaScript code

 jQuery method is used to post the target’s credentials to hosting site Figure 9. jQuery method is used to post the target’s credentials to hosting site

The phishing pages record passwords inputted by site visitors. Once the compromised credentials are used to successfully log in to accounts, fraudsters can identify themselves as executives. They will then send a fraudulent wire transfer request to trick recipients into wiring money into the criminals’ accounts.

We found a BEC mail sample that was sent from the same IP. The email in question is an invoice request that has a legitimate email header, which is a known tactic used in BEC scams.

 An email sample with the same originating IP Figure 10. An email sample with the same originating IP

 A sample fake PDF invoice in a BEC email Figure 11. A sample fake PDF invoice in a BEC email

How to defend against BEC and other phishing scams

Unlike other cybercriminal schemes, [phishing](#) and [BEC scams](#) can be tricky to detect as they are targeted toward specific recipients. Attackers seek to compromise email accounts to gain access to financial and other sensitive information related to business operations.

Here are some tips on how to stay protected from email scams:

- **Educate and train employees.** Deflect company intrusions through InfoSec education. All staff — from the CEO to rank-and-file employees — must learn about the different kinds of scams and what to do in case of any encounters (i.e., double-check with others and verify email details).
- **Confirm requests using other channels.** Exercise caution by following a verification system (e.g., multiple signoffs or additional verification protocols) among employees that work with sensitive information.
- **Scrutinize all emails.** Be wary of irregular emails with suspicious content such as dubious sender email, domain name, writing style, and urgent requests.

In the case discussed here, the attacker email itself does not include the typical malware payload of malicious attachments. As a result, traditional security solutions won't be able to protect accounts and systems from such attacks. Users can also turn on mail inspection for sender "sendgrid[.]net" in the email gateway.

Trend Micro protects both small- to medium-sized businesses and enterprises against phishing- and BEC-related emails. Using enhanced machine learning combined with expert rules, [Trend Micro™ Email Security](#) solution analyzes both the header and the content of an email to stop BEC and other email threats. For source verification and authentication, it uses Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-Based Message Authentication, Reporting and Conformance (DMARC).

The [Trend Micro™ Cloud App Security](#) solution enhances the security of Microsoft Office 365 and other cloud services through sandbox malware analysis for BEC and other advanced threats. It uses Writing Style DNA to detect BEC impersonations and computer vision to find credential-stealing phishing sites. It also protects cloud file sharing from threats and data loss by controlling sensitive data usage.

Indicators of compromise (IOCs)

Threat actor-managed C&C URLs:

- [https://highstreetmuch\[.\]xyz/hug/gate\[.\]php](https://highstreetmuch[.]xyz/hug/gate[.]php)
- [https://takeusall\[.\]online/benzz/gate\[.\]PHP](https://takeusall[.]online/benzz/gate[.]PHP)

MITRE ATT&CK® Matrix

 Water Nue MITRE ATT&CK Mapping