Phishing Campaign Report

Date: 7.3.2024

Time: 7:00-22:45

Target: CEITEC at Masaryk University

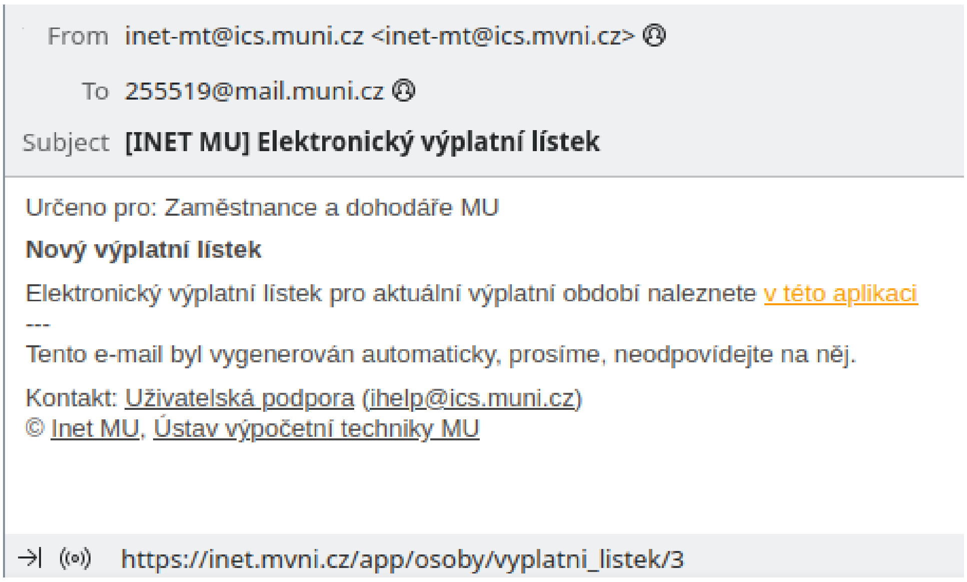
Summary

We have executed a training phishing attack using a spoofed version of a pay slip notification. This notification is sent regularly from the INET system. We have intentionally chosen the morning of the day the notification would normally arrive. We have found that almost **49% of the targeted staff clicked** on the phishing link, **more than 35% provided their password**, and only 10 of them had multi-factor authentication enabled. However, TOTP second factor was provided in all these cases. The recommended steps to mitigate this threat are described at the end of the document.

This was a second iteration of the same phishing vector. In the first iteration that took place in September 2023, **39**% of recipients provided their password. Although there has been a slight improvement, the resulting figures are still alarmingly high.

Setup

We bought a domain `mvni.cz` for this attack because it is similar to `muni.cz`. We set up a simple mail infrastructure using a virtual server in OpenStack with domain name outsider.csirt.muni.cz and IP address outside the MUNI range of 147.251.0.0/16. We set up SPF, DKIM and DMARC to increase the credibility of the email. The email was an exact copy of the original Czech version with added spoofed sender's name to fool mobile clients more easily. Each message also contained a unique tracking link to https://inet.mvni.cz/app/osoby/vyplatni_listek/.



From inet-mt@ics.muni.cz <inet-mt@ics.mvni.cz>

To 255519@mail.muni.cz

Subject **[INET MU] Elektronický výplatní lístek**

Určeno pro: Zaměstnance a dohodáře MU

Nový výplatní lístek

Elektronický výplatní lístek pro aktuální výplatní období naleznete v této aplikaci

---

Tento e-mail byl vygenerován automaticky, prosíme, neodpovídejte na něj.

Kontakt: Uživatelská podpora (ihelp@ics.muni.cz)
© Inet MU, Ústav výpočetní techniky MU

https://inet.mvni.cz/app/osoby/vyplatni_listek/3

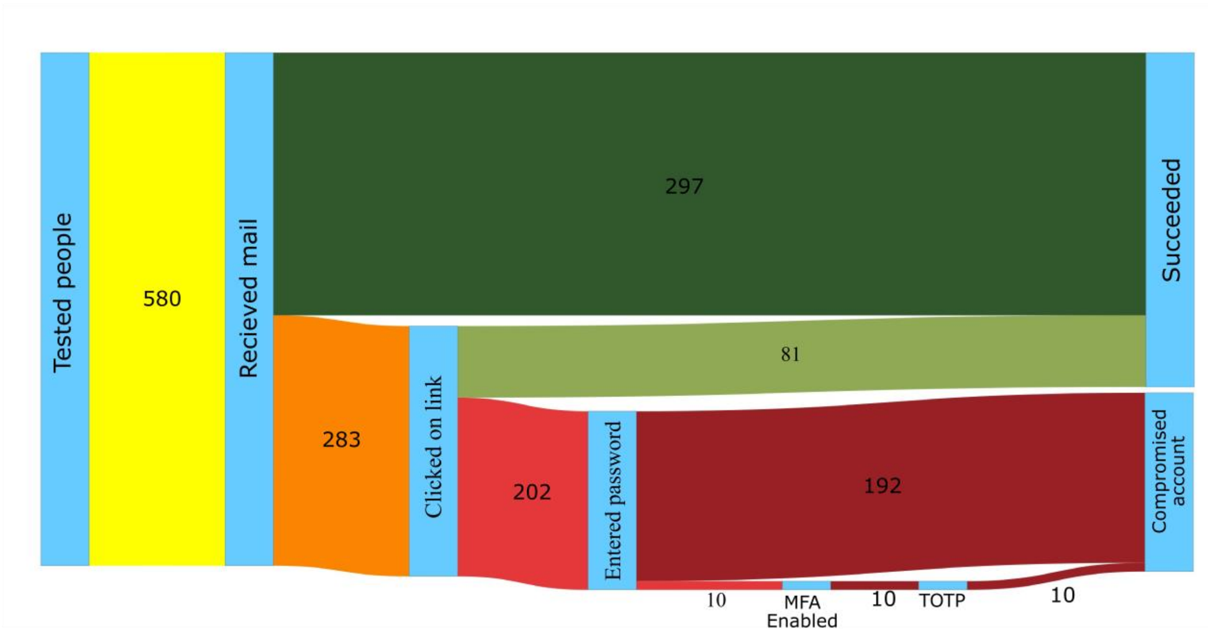
We created a copy of the SSO login page at `id.mvni.cz` and redirected the request to this page. This page collected information about provided credentials (tracking id, password length, TOTP, and login validity).

If the user did not have MFA enabled or entered correct TOTP code, he was redirected to a landing page explaining the campaign.. If a user attempted to use a security key on the malicious login page, he was presented with an error message which suggested that another type of second factor should be tried.

Results

Out of the 580 tested people, 283 (almost 49%) clicked the link included in the email. 202 people (35%) entered their password, 10 of those had MFA already set up. However, valid TOTP was entered by all these people. 202 accounts were compromised in total. The data are visualized in the graph below.

When a phishing email is encountered, users are encouraged to report it to CSIRT-MU. In this case 6 reports were made to CSIRT-MU in total. 14 more reports were made using O365 report mail feature.



50% of passwords were entered from an IP address from networks other than 147.251.0.0/16 which suggests that people are accessing INET from their mobile devices and homes. We have observed 41 logins from Android phones and 32 from iPhones. As for PCs, there were 12 Linux machines and 108 Windows machines. Users often entered their valid passwords from multiple devices and IP addresses. The total number of valid passwords entered was 287. There were also 89 invalid login attempts.

After providing a valid password to the phishing site, users were redirected to https://security.muni.cz/en/phishing/pay-slip where the campaign is explained and recommendations provided. There were 45 users that interacted with the page (by clicking on some of the links).

We have been able to successfully phish the primary login password of 35% of the targets with an attack that did not require any specialized tools. The total cost of this attack for an attacker is less than 200 CZK for the domain and a few hours of his time to set up the campaign. Target email addresses can be easily gathered from the public web https://www.muni.cz/en/about-us/organizational-structure.

Impact

The impact of such a simple phishing attack can be extremely high, especially for a research institute, where some of the accounts have access to sensitive research data. The attacker can misuse gained access to many services, including email, o365 OneDrive, SharePoint, data storage and others. A secondary password for VPN and Eduroam networks can be revealed in plaintext in IS, which would allow an attacker to access the internal MU network.

Recommendations

The people targeted in this attack mostly did not have MFA set up. In our experience, using MFA with TOTP second factor does not protect the users adequately as they simply enter the TOPT to the phishing login form as well, which gives an attacker access to this account from a given device. This was also demonstrated by the 10 users who provided us with valid TOTP. To counter this threat, the domain to which the credentials are entered needs to be verified. If the verification is left to the user, it will inevitably fail. Therefore, we recommend the use of **security keys** for authentication, which are cryptographically guaranteed to perform the verification correctly.

Platform security keys and passkeys

All major platforms (Windows with Windows Hello, macOS and iOS/iPadOS, Linux with tpm-fido, Android) support a combination of platform keys and/or passkeys that can be used as FIDO2 security keys. Moreover, passkeys make it possible to use mobile devices for cross-platform authentication. Users in possession of supported devices should be encouraged to enroll the token provided by their operating systems and use it exclusively.

Hardware security keys

If a software security key is not available, a hardware token can be obtained for a price as low as 500 CZK. It can be used on multiple devices and for multiple services as well.

More information can be found at https://perunaai.atlassian.net/wiki/spaces/PERUN/pages/198803530/Multi-factor+Authentication.

Password managers

Users should be encouraged to use password managers. There are two main advantages to doing so. The first is that it is easier to have longer and stronger passwords when the user is not required to remember them. It also helps to prevent password reuse, which is a problem when a password is compromised on one service and then used to attack another. It also makes it easier to create a new password when the old one is compromised. The second advantage is that, in combination with browser extensions, the password manager can fill in passwords for known websites. This makes it more convenient for the user, and it can also help to mitigate phishing since the extension will check the website domain name before filling in the credentials.