Phishing has been a prominent cyber threat for decades, stealing the spotlight as the most prevalent attack vector for years, but the latest breed of attacks is more sophisticated and complicated to protect against than ever before. Attackers are always looking for new techniques to bypass security measures and remain undetected by victims. In the past year, Browser-in-the Browser (BITB) attacks have emerged as a very effective technique for evading detection and convincing users to hand over credentials. Zscaler first observed a phishing campaign using this technique back in February of 2020. Early this year, an unaffiliated security researcher who goes by the handle mrd0x on Twitter, took to the social platform to share key technical details revealing how this technique takes advantage of third-party single sign-on (SSO) targeting brands like Apple, Microsoft, and Google. Most commonly, BITB attacks mimic single sign-on (SSO) windows with mostly undetectable fakes of the familiar log-in pop-ups.

Underlining this trend, the Zscaler ThreatLabz team recently observed a new Browser-in-the Browser (BITB) attack impersonating an Indian government website to deliver a sextortion demand with the threat of releasing sensitive information about victims if they refuse to pay. This layered phishing attack appears to be the first of its kind, delivering a pop-up window that states a victim's browser is blocked due to repeated visits of pornographic websites prohibited by the Government of India. Attackers then prompt the victim with an extortion demand requiring them to enter a credit card and pay a fine to avoid being arrested by the police.

The homepage of this scam depicts a notice from the Indian government that due to repeatedly visiting pornographic sites user's browser is blocked and asks users to pay a fine by entering their card details. The mechanism by which the scam link is delivered to the victims is still unknown, but our research indicates that this may be linked to a landing page pop-up with a common alert that the user is about to leave the current page without saving the changes. This type of alert window, shown below in Fig 1 typically pops-up on legitimate websites when a user tries to close a form tab without saving or submitting entered data.

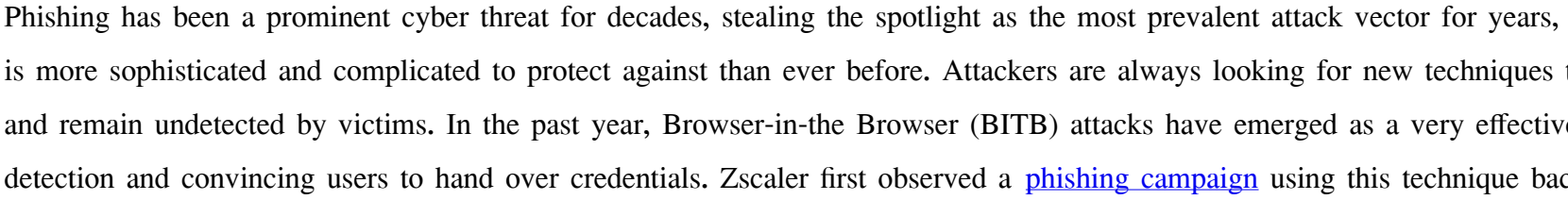

Fig 1: Initial pop-up alert window before fullscreen

Regardless of whether the victim clicks on the Leave or Cancel button the browser switches to full-screen mode. In this mode the scam becomes more difficult for most victims to recognize because normally when we switch the browser in full screen the address bar will disappear but in this case, there is a fake address bar which looks like a normal site in the browser and is very hard to identify as fake.

Once the fake browser window expands into full-screen mode it also appears to have all the same icons and buttons of a legitimate browser as shown in the Fig 2 screenshot below.

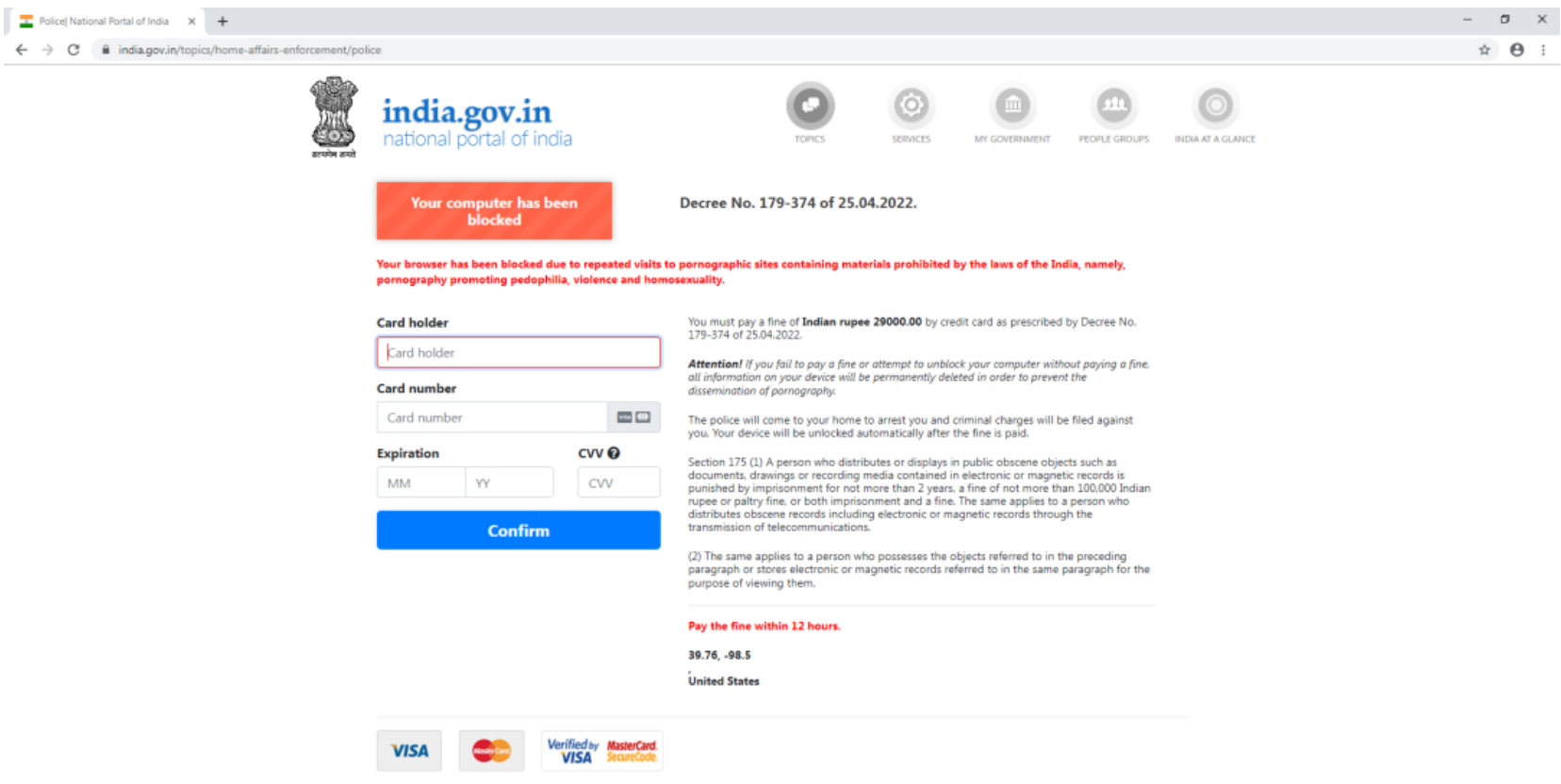

Fig 2: Fake India gov page with a full-screen window

Of note, from this window, the address bar, minimize button, maximize button, refresh and back button are all fake and un-clickable, and the user is unable to select and drag to move or resize the window. The screenshot in Fig 3 below shows that if the user moves the mouse to the top of the browser window the closing icon will popup confirming the window is in full-screen mode.

For the vigilant user or researcher, this is a clear indication BITB attack that reveals the open browser window is trying to hide the real URL and prevent the user from navigating away from the fake page.

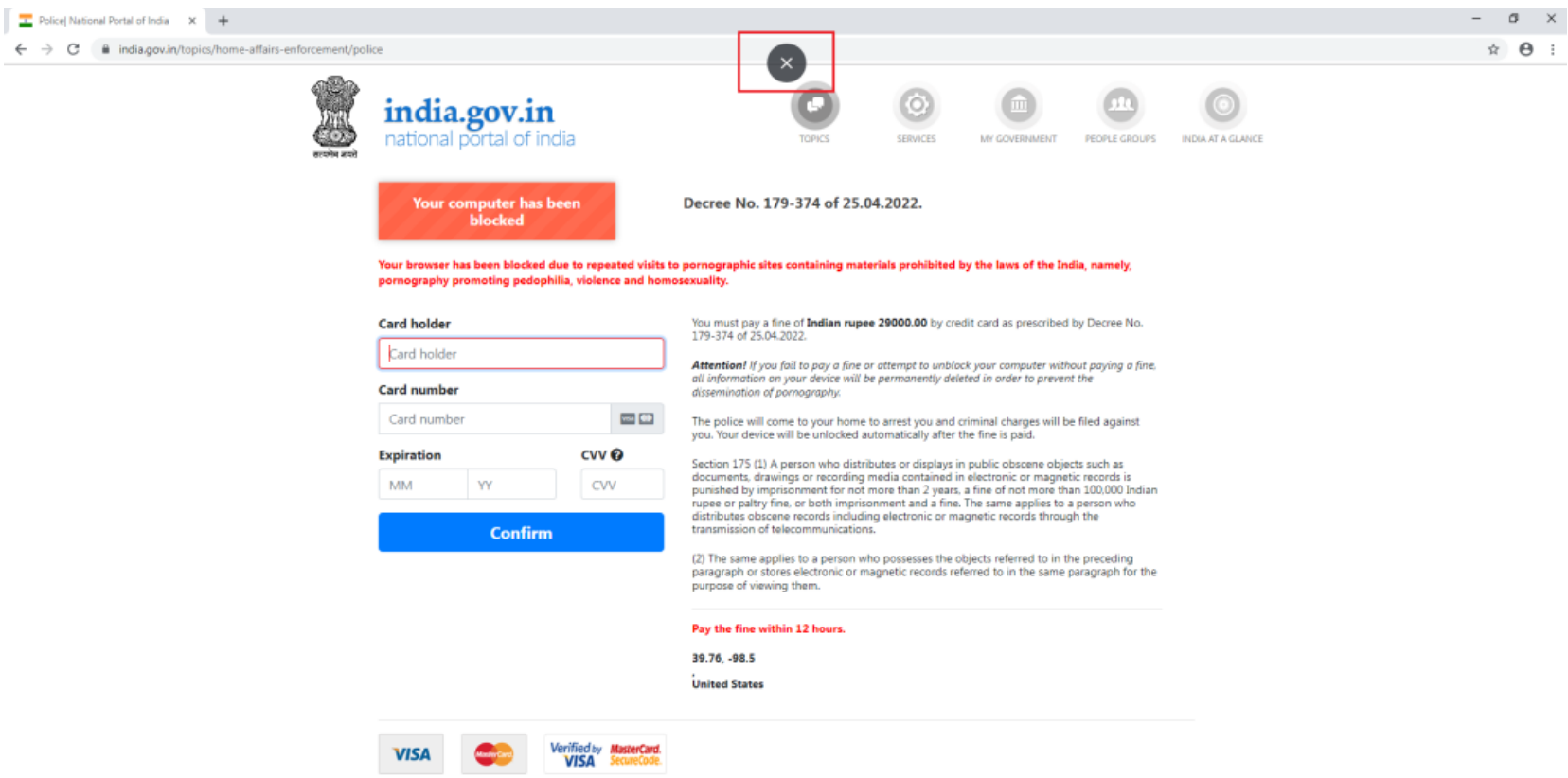

Fig 3: Window with a close popup button

After exiting the full-screen window, it can be clearly seen in the below screenshot (Fig 4) that there are two address bars. The top address bar is the actual browser with the malicious website address and the below address bar is the fake address bar with buttons as images, and are loaded from the following URLs.

supernight[.]world/assets/img/header_1.png (URL Image)

supernight[.]world/assets/img/header_3.png(Close, Minimize, and maximize image)

Window after exiting the full-screen mode.

Fig 4: Window after exiting the full-screen mode.

Attackers use browser fingerprinting, shown in Fig 5, and query browser attributes to create hashed visitor identifiers. This is a critical step in the attack because a browser's unique fingerprint data remains the same in incognito/private mode and when browser data like cookies and local storage is purged. This means that the attacker can still track the victim and carry out attacks even when users are taking extra safety precautions like using incognito browsers and purging site cookies.

Browser fingerprinting.

Fig 5: Browser fingerprinting.

The browser fingerprinting data is sent to the server and if it returns with success flag as false, the user is either redirected to the hardcoded redirected domain i.e. hxxps://google[.]com/. If the browser fingerprinting data is sent to the attacker successfully then the server responds with a success flag and along with that responds with the credit card payment form code and SMS/ OTP form, shown in Fig 6.

Response from the server with fake credit card and SMS details form.

Response from the server with fake credit card and SMS details form.

Fig 6: Response from the server with fake credit card and SMS details form.

Any action by the victim on the scam page like scroll, mouse event or keypress will result in moving focus to the credit card details fields, shown in Fig 7.

Function to set focus to credit card details field.

Fig 7: Function to set focus to credit card details field.

After the user submits their credit card information, the scam site redirects to the payment processing window and prompts the victim to wait and tells them that their payment is being processed and not to close the page, however, this processing screen never updates or indicates when the transaction is completed, shown in Fig 8.

Payment processing window after submitting credit card information

Fig 8: Payment processing window after submitting credit card information

The attacker verifies the credit card credentials entered by the user and the page will not accept invalid card details, as shown in Fig 9.

Credit card validation

Fig 9: Credit card validation

After the extorted credit card details are validated, the credentials are sent to URL hxxps://supernight[.]world/gateway.php, shown in Fig 10.

Sending stolen credit card credentials to c2 location

Fig 10: Sending stolen credit card credentials to c2 location

Technical Appendix:

This phishing page also has anti-debugging techniques, if the phishing kit is being deployed locally then the browser will not switch to the fullscreen mode.

Function to switch browser to full-screen mode

Fig 11: Function to switch browser to full-screen mode

Function to disable the below keystrokes:

F1-F10, Tab, Enter, Caps lock, Insert, Page Up-Down, End, Home, Arrow Left-Up-Right-Down, Print Scrn, scroll lock and right-left window key

Disable keystrokes

Fig 12: Disable keystrokes

All mouse events will call the setfocus function.

Fig 13: All mouse events will call the setfocus function.

Indicators of compromise

supernight[.]world alimalipay[.]xyz searchfirst[.]xyz secondsearch[.]xyz centralthis[.]xyz smemepay33[.]xyz npepayse17[.]xyz smemepay36[.]xyz npepayse21[.]xyz smemepay37[.]xyz smemepay29[.]xyz weserv38573w14[.]xyz weserv38573w9[.]xyz weserv38573w8[.]xyz vvservnkren8[.]xyz mmpepay16[.]xyz mmpepay12[.]xyz mmpepay19[.]xyz npepayse20[.]xyz desctopfree[.]xyz smemepay37[.]xyz npepayse19[.]xyz smemepay33[.]xyz smemepay36[.]xyz npepayse21[.]xyz npepayse17[.]xyz smemepay29[.]xyz weserv38573w14[.]xyz weserv38573w9[.]xyz weserv38573w8[.]xyz

65.20.70[.]213 92.255.85[.]133

Other adult redirection and scam domains resolving to the same IPs (possibly related to this campaign) supernight[.]xyz jerkdolls[.]digital jerkdolls[.]xyz jerkdolls[.]shop istripper[.]world istripper[.]online istripper[.]bond istripper[.]shop istripper[.]info istripper[.]icu weppahgeje5[.]xyz npepayse20[.]xyz smemepay35[.]xyz npepayser9[.]xyz smemepay34[.]xyz npepayse22[.]xyz smemepay28[.]xyz smemepay27[.]xyz smemepay20[.]xyz smemepay25[.]xyz vvservnkren10[.]xyz smemepay26[.]xyz smemepay24[.]xyz weserv38573w11[.]xyz tttsertkfm6[.]xyz tttsertkfm5[.]xyz tttsertkfm4[.]xyz

vvservnkren18[.]xyz weserv38573w19[.]xyz fooldating[.]xyz weserv38573w10[.]xyz fooldat1ng[.]xyz desctopfree[.]xyz weserv38573w17[.]xyz vvservnkren1[.]xyz weserv38573w12[.]xyz weserv38573w13[.]xyz

- Security Research
- Insights and Research
-

Authors

Kaivalya Khursale

Prakhar Shrotriya

Recommended for You

Vidar distributed through backdoored Windows 11 downloads and abusing Telegram

Peeking into PrivateLoader

Targeted attack on Thailand Pass customers delivers AsyncRAT

A "Naver"-ending game of Lazarus APT