Lookout discovers phishing site targeting DNC

Further investigation by the DNC has revealed that this was an unsanctioned simulated test. Lookout's artificial intelligence successfully detects phishing threats independent of the source of such exploits.

As reported by The Washington Post and CNN, Lookout discovered a custom phishing kit targeted at the Democratic National Committee (DNC) via a third-party technology provider NGP VAN.

Upon finding this website, Lookout immediately informed the DNC, NGP VAN, and the hosting provider DigitalOcean. All teams promptly acted to investigate and take down the identified phishing domain. More details on these events are provided below.

How Lookout detected this phishing kit

Lookout built our artificial intelligence-based phishing detection engine with the intent of discovering and detecting phishing sites as early as possible in the attack lifecycle - ideally, before the attacker is able to send out messages targeting users. Our AI engine discovered and alerted on this site as a custom phishing site, and our Principal Engineer for phishing, Jeremy Richards, started to investigate the site, which was hosted on DigitalOcean's infrastructure. This phishing site replicated a login page for a technology provider, NGP VAN, which is primarily used by the United States Democratic Party, Democratic campaigns, and other non-profit organizations authorized by the Democratic Party.

As the Lookout investigation progressed, we reached out to the DNC, NGP VAN, and DigitalOcean so that they could each initiate their own response workflows. Within hours of Lookout contacting these organizations, DigitalOcean had taken down the phishing site before any messages were able to be sent by the attacker.

Detailed timeline of events

1. Less than 30 minutes after the site goes live, Lookout's machine learning identifies the domain "accounts[.]ngpvan[.]verifyauth[.]com" as "high risk" of being a phishing website. The flagged site is sent to researchers for further review.

Figure 1: *Flagged message sent to researchers.*

2. Jeremy Richards starts a manual investigation and determines the site is hosted at DigitalOcean. At this point, the site is simply a "welcome" page:

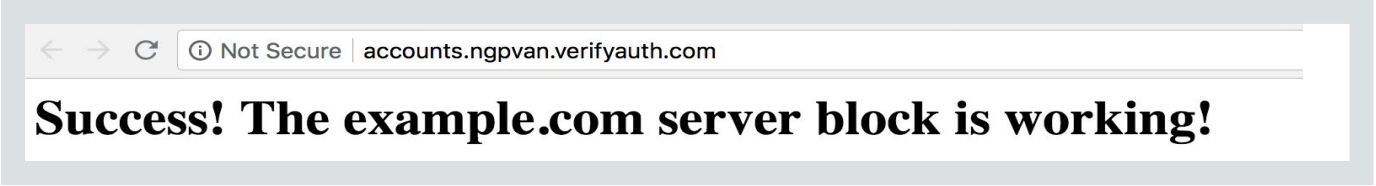

Figure 2: *Initial message displayed on the site while it's under development.*

The message indicates the website is not currently set up as an active phishing campaign, but based on the confidence that the AI-based phishing engine has, Jeremy continues to monitor the infrastructure.

3. Only an hour later, the site evolves, taking on a login screen and details about "ActionID" and "NGP VAN". The Lookout team determines that Action ID, which is created by NGP VAN, is the login page for the backend of NGP VAN and may be a fertile method for stealing campaign-related data. We immediately prioritize this investigation and start looking for contacts at NGP VAN, DigitalOcean and DNC.

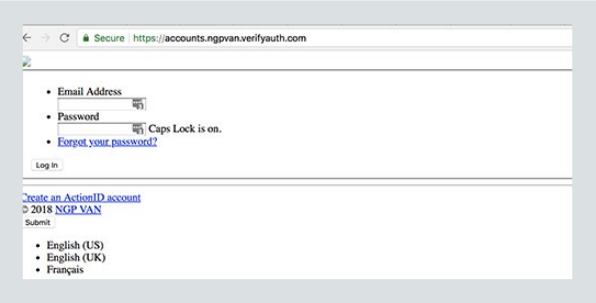

Figure 3: *As Lookout monitors the site, we observe it is under active development and is evolving into a functional phishing login page.*

4. We continue to monitor the actively developing site. Within a half hour, it evolves into a designed, fake version of "Action ID," clearly meant to phish someone who would typically access the NGP VAN site on a laptop or mobile device.

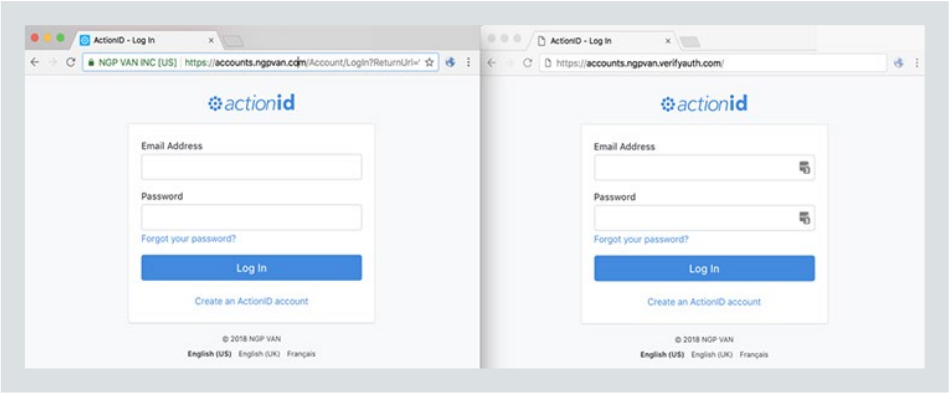

Figure 4: *The phishing site ultimately evolves into a convincing spoof of the original Action ID site. Real website seen on left, phishing site seen on right.*

5. We contact representatives from DNC, NGP VAN and DigitalOcean to notify them of the presence of this phishing site. NGP VAN and DigitalOcean respond immediately — NGP VAN even went so far as to confirm that our notification wasn't actually part of a larger elaborate phishing campaign. DNC responds shortly after and all teams get on a late night / early morning conference call to coordinate investigation and the takedown.

6. The phishing site is taken down and the investigation is handed off to NGP VAN, DigitalOcean, and the FBI.

Phishing in a new era of security

Lookout offers artificial intelligence-based phishing detection as part of the recently launched Phishing and Content Protection solution that is currently in use by certain enterprise and government customers of Lookout Mobile Endpoint Security.

Lookout has found that all kinds of devices are susceptible to such phishing attacks. Attackers specifically look to target organizations that have a "mobile workforce," or employees and volunteers who work on multiple devices and are located in a wide variety of locations.

Modern devices are evolving in their risk posture, as users receive communications through an increasing number of channels. Where as organizations used to only have to protect against email-based phishing attacks, modern phishing attacks now occur through a variety of means: email, SMS, extended SMS messengers like Apple Messages, Google Hangouts, WhatsApp, WeChat, and social media sites like Facebook, LinkedIn, etc. Endpoints are constantly in motion from Wi-Fi to mobile networks, leaving the devices often unprotected and outside the organization's security perimeter. These dynamics have created fertile ground for attackers to use phishing attacks to compromise organizations.

To learn more about how to prevent phishing attacks at your organization, contact Lookout today.