SNAPSHOT

THE MEDIA TRUST
We know digital security.

Digital Trends: July 2020

Continuously morphing ICEPick-3PC malvertising attack penetrates ad blocking defenses.

Key Learnings

- Attack vector changed tactics to extend reach
- Changing domain patterns helped attack evade malware blockers at both ad tech providers and publishers
- Recommendations:
  - Client-side scanning to detect evolving patterns
  - Continuous updating of malware block list data

The month of July bore witness to a persistent malvertising attack affecting more than 100 digital properties from more than 50 publisher groups across the U.S., UK and Germany. The multi-step campaign showcased the stealthy and evolving sophistication of the attackers to bypass malware blockers and manipulate standard third-party ad serving platforms in order to defraud consumers via phishing schemes or unwanted adware installation.

Changing tactic proves effective

This type of tactic is not new—ICEPick-3PC was first detected in October 2018, reaching significant mass in January 2019—but it has been changing throughout 2020. Initially, the tactic involved small DSPs targeting mobile users at local publications. These smaller campaigns were sporadic, launching every other weekend and using obvious domains that were easy to block. Gradually, the attack evolved to encompass more domains, and the emerging domains—many newly-created—drove the creation of new incidents or events. [Figure 1]. In addition, their dynamic nature means these domains are not readily picked up by malware blockers that rely on static or third-party lists.

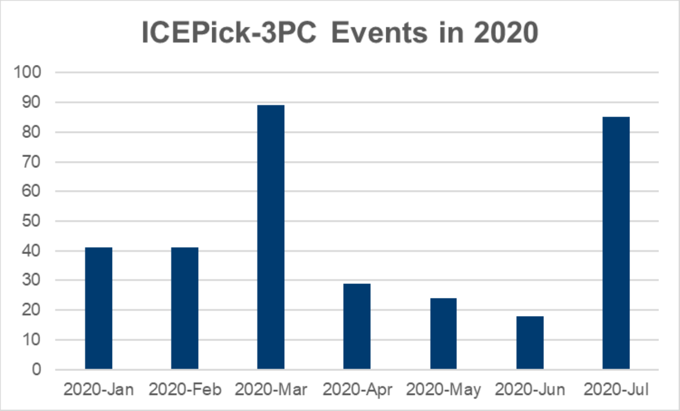

Figure 1: Maturing attack drives more events affecting larger group of ad tech platforms and publishers

© 2020 The Media Trust

The July surge of attacks exhibited three significant differences compared to earlier events:

- **Targeting criteria**: Changed from mobile Android users to target desktop Chrome browsers
- **DSP scale**: Leveraged bigger, more reputable DSP platforms to gain access to more premium publishers and their larger user base, i.e., more readers equals more victims
- **Attack Length**: Related to the above, more reputable DSPs readily responded to notifications and quickly isolated and removed offending buyers from their platforms, thereby shortening the attack cycle from several days to hours. However, the reach was significant.

Breaking down the attack

Isolated to buyers on self-serve ad platforms, this attack leveraged the platform's pre-loaded interactive web content and animation tools to redirect and exfiltrate device and sensitive user information. Creating a seat on Wednesday, July 22, and trafficking clean campaigns to access several premium DSPs, the buyer changed the campaign code a few days later, in the early morning hours (Eastern Standard) on Saturday, July 25. The code targeted Chrome browsers and once the device was identified, launched one of two payloads: phish for user information or malware auto-installation. [Figure 2]

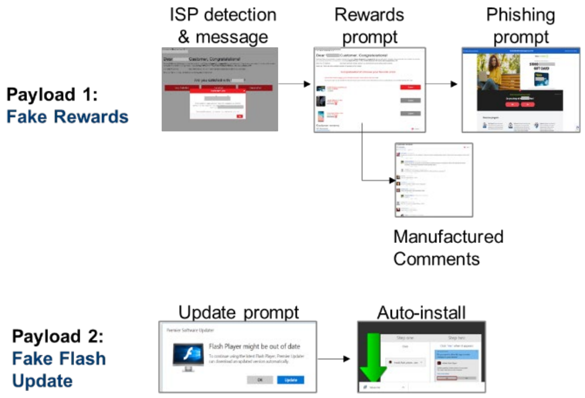

Figure 2: Anatomy of the two-payload attack

Upon successful detection of an ISP, the consumer is served an ISP-specific message offering multiple rewards. Adding legitimacy and urgency, the page listed dozens of manufactured consumer comments and indicates only one reward option remains, a gift card at a well-known retailer.

If the ISP is not detected consumers are prompted to update their Adobe Flash which auto-installs the malicious payload.

Within minutes of detecting the code change, The Media Trust alerted impacted clients, fed the emerging attack vectors to Media Filter (our malware blocking tool), and began investigation to shut down the attack at the source. The primary DSPs confirmed account termination—one within 6 hours, the second in 12 hours, and the third in 48 hours.

Quickly changing structure requires comprehensive approach

This attack (and a subsequent smaller scale attack the first weekend of August) successfully bypassed malware blockers not able to keep up-to-date with the changing vectors on both ad tech providers and media publishers, including two premium UK publishers. The scale, sophistication, repetition, and reach led to active discussions in the TAG super user group and The Media Trust's active collaboration with authorities.

Malware attacks are inevitable; no one is guaranteed a malware-free existence. However, there are a few steps to mitigate an attack's success. Tactics to address this type of rapidly evolving attack include:

- **Scanning**: Continuous scanning via profiles covering a diverse set of geographies, user agents, and devices
- **24/7/365 malware coverage**: Strong, experienced team of malware experts constantly analyzing data in order to detect the attack as it emerges
- **Scanning-informed Blocker**: Malware blocker fed with up-to-the-minute malicious domain, url, and host data derived from scanning
- **Partner collaboration**: For attacks that linger or repeat, contact your upstream partner and request confirmation that the offender has been removed and/or their seat terminated.

© 2020 The Media Trust