This report is provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. The DHS does not endorse any commercial product or service, referenced in this bulletin or otherwise.

This document is marked TLP:WHITE. Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction. For more information on the Traffic Light Protocol, see http://www.us-cert.gov/tlp/.

Summary

Description

This Malware Analysis Report (MAR) is the result of analytic efforts between the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI). Working with U.S. Government partners, DHS and FBI identified Trojan malware variants used by the North Korean government - referred to by the U.S. Government as BANKSHOT. The U.S. Government refers to malicious cyber activity by the North Korean government as HIDDEN COBRA. For more information on HIDDEN COBRA activity, visit https://www.us-cert.gov/hiddencobra.

FBI has high confidence that HIDDEN COBRA actors are using malware variants in conjunction with proxy servers to maintain a presence on victim networks and to further network exploitation. DHS and FBI are distributing this MAR to enable network defense and reduce exposure to North Korean government malicious cyber activity.

This MAR includes malware descriptions related to HIDDEN COBRA, suggested response actions and recommended mitigation techniques. Users or administrators should flag activity associated with the malware, report the activity to the DHS National Cybersecurity and Communications Integration Center (NCCIC) or the FBI Cyber Watch (CyWatch), and give the activity the highest priority for enhanced mitigation.

This report provides analysis of seven (7) malicious executable files. Five (5) of these files are proxy applications that all use a similar cipher algorithm to mask traffic between the malware and the remote operator. Additionally, two of the five proxies have the ability to generate fake TLS handshake sessions using valid public SSL certificates, disguising network connections with remote malicious actors. The remaining two (2) executables are remote access tools (RATs), providing remote users with the ability to run various commands on an infected system. One of these RATs uses a cipher and the OpenSSL library to add a layer of encryption to communications between the infected system and its command and control (C2) server; this RAT may have been used to install the proxy servers onto compromised systems.

The following YARA signature can be used to detect the proxy servers and RATs:

rule Unauthorized_Proxy_Server_RAT
{
    meta:
        Author="US-CERT Code Analysis Team"
        Incident="10135536*
        MD5_1 = "C74E289AD927E81D2A1A56BC73E394AB"
        MD5_2 = "2950E3741D7AF69E0CA0C5013ABC4209"
        Info="Detects Proxy Server RAT"
    super_rule = 1
}

strings:
$s0 = {8A043132C288043125FF00000003C299F73D40404900A14440490003D0413BCF72DE5E5FC3}
$s1 = {8A0431884421432C28804318B44241425FF00000003C299F73D40404900A14440490003D0413BCF72DE5E5FC3}
$s2 = {8A0431884421432C28804318B44241425FF00000003C299F73D5C394100A16039410003D0413BCF72DE5E5FC3}
$s3 = {8A0431884421432C28804318B44241425FF00000003C299F73D5C394100A16039410003D0413BCF72DE5E5FC3}
$s4 = {B91A790008A140780F29A8810404975F4}
$s5 = {399FE192769F839DCE9F2A9D2C9EAD9CEB9FD19CA59F7E9F539CEF9F029F969C6C9E5C9D949FC99F}
$s6 = {8A0431884421432C28804318B44241425FF00000003C299F73D4060009010A144600910003D0413BCF72DE5E5FC3}
$s7 = {3C5C75208A41014184C074183C72740C3C7474083C6274043C2275088A41014184C075DC}$
$s8 = {8B063D9534120077353D59341200722E668B4604663DE8037F24}$
$s9 = {8BC88B74241CC1E1052BC88B7C241BC1E10488B5C24140C86D04888B4C242083F9018944240C7523}$
$s10 = {8B063D9034120077353D59341200722E668B4604663DE8037F246885C0}$
$s11 = {30110FB60148FFEC0102C20FBEC09941F7FF94103D249FF875E7}$
$s12 = {448BEB88FEECC44E41F7EDC1FA038BCAC1E91F03D16BD21A442BEA4183C541}$
$s13 = {8A0A80F9627C2380F9797F1E80F9647C0A80F96D7F0580C108EB0D80F96F7C0A80F9787F05}$

condition:

any of them

<table>
<thead>
<tr>
<th>Files</th>
<th>Processed</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>7</td>
</tr>
<tr>
<td></td>
<td>0137f688436c468d43b3e50878ec1a1f (0137F688436C468D43B3E50878EC1A1F)</td>
</tr>
<tr>
<td></td>
<td>114d8db4843748d79861b49943c8b7ca (114D8DB4843748D79861B49943C8B7CA)</td>
</tr>
<tr>
<td></td>
<td>2950e3741d7a6f69e0ca0c5013abc4209 (2950E3741D7AF69E0C0C5013ABC4209)</td>
</tr>
<tr>
<td></td>
<td>964b291ad9bafa471da3f80f8262d8e7 (964B291AD9BFA471DA3F80F8262D8E7)</td>
</tr>
<tr>
<td></td>
<td>9e4d9ed07c348b10863d89b6bb08141 (9E4D9EDB07C348B10863D89B6B08141)</td>
</tr>
<tr>
<td></td>
<td>c74e289ad927e81d2a1a56bc73e394ab (C74E289AD927E81D2A1A56BC73E394AB)</td>
</tr>
<tr>
<td></td>
<td>fc9e40100d8f0f80f303a3414f50ec (FC9E40100D8FAE2DF0F30A3414F50EC)</td>
</tr>
</tbody>
</table>
### C74E289AD927E81D2A1A56BC73E394AB

**Details**
- **Name**: C74E289AD927E81D2A1A56BC73E394AB
- **Size**: 675840
- **Type**: PE32 executable (GUI) Intel 80386, for MS Windows
- **MD5**: c74e289ad927e81d2a1a56bc73e394ab
- **SHA1**: 771f7d69a476d5b0b7c942bdc21e86691dabba89
- **ssdeep**: 12288:NxZ0n+1OzKZDK+xgYDUWFVBXfJzLrpooqR:a+EzUFVUNIPz9poq
- **Entropy**: 6.65567602919

**Antivirus**
- **K7**: Trojan (700000041)
- **Cyren**: W32/Heuristic-KPPEldorado
- **VirusBlokAda**: BScope.Trojan.Agent

**PE Information**
- **Compiled**: 2016-06-21T05:56:00Z

**PE Sections**
- **Name**: (header)
  - **MD5**: f4c5b7ebe0ff8b8c5d5632877552f2e23
  - **Raw Size**: 4096
  - **Entropy**: 0.649735689975
- **Name**: .text
  - **MD5**: d2cf27a072c85308a12b834aa3150af0
  - **Raw Size**: 442368
  - **Entropy**: 6.63294155589
- **Name**: .rdata
  - **MD5**: bc433c07b82c684a09d26e014c0ce0d
  - **Raw Size**: 159744
  - **Entropy**: 6.13100276138
- **Name**: .data
  - **MD5**: 1cfe81260eb717a1b917d7b3d1349851
  - **Raw Size**: 69632
  - **Entropy**: 4.94697538055

**Packers**
- **Name**: Microsoft Visual C++ v6.0
- **Version**: NA
- **Entry Point**: NA

**Description**
This artifact is a malicious PE32 executable that allows a remote operator or a server to perform various remote operations. When executed, the malware binds to the victim system and listens to activity on port 110. Static analysis of this application indicates that its primary purpose is to force a compromised system to function as a proxy server for Internet connections. This capability enables an operator to securely access the Internet through the compromised host. Data to and from the victim system is encoded to prevent identification of the proxy sessions by firewalls or network analysis devices.

Analysis of the cipher algorithm indicates it uses a four-byte key. When the compromised system operating as a proxy server receives an initial connection from the operator, it expects to receive the four-byte key. The malware accepts six additional bytes, which are decoded by using the cipher and the previously received four bytes. The malware verifies the first four bytes received from the operator are between the values 00123459h and 00123490h. If the first four bytes do not fall between these values, the malware terminates the session with the operator. If the first four of these six bytes are between the specified values, the malware accepts the additional data. From the previous six bytes of data, the fifth and sixth byte are used to make up a double word value, which is used to identify the size of the data the malware expects to arrive next. If the double word value is larger than 1,000 bytes, the malware will terminate the connection. Analysis indicates this is a safety mechanism built into the software to protect it from buffer or heap sprays.

### FC9E40100D8FAE2DF0F30A3414F50EC

**Details**
- **Name**: FC9E40100D8FAE2DF0F30A3414F50EC
- **Size**: 684032
- **Type**: PE32 executable (GUI) Intel 80386, for MS Windows
- **MD5**: fc9e40100d8fae2df0f30a3414f50ec
- **SHA1**: 566243e09a3d19828c243c799f638ae34469d967
- **ssdeep**: 12288:DLvM82yKa7LYISZJMcHs82mdQlQYIFph:ziQi82gQH4ph
- **Entropy**: 6.622634126
**Antivirus**

- Cyren: W32/Heuristic-KPP\Eldorado
- VirusBlokAda: BScope.Trojan.Agent

**PE Information**

- Compiled: 2016-04-24T01:55:11Z

**PE Sections**

<table>
<thead>
<tr>
<th>Name</th>
<th>MD5</th>
<th>Raw Size</th>
<th>Entropy</th>
</tr>
</thead>
<tbody>
<tr>
<td>(header)</td>
<td>a679879146f59c7ba1b29ff42851a5ed</td>
<td>4096</td>
<td>0.627951249971</td>
</tr>
<tr>
<td>.text</td>
<td>d25e32c2f4c243f8b0f537b73c6f07c</td>
<td>442368</td>
<td>6.65458990149</td>
</tr>
<tr>
<td>.rdata</td>
<td>b94f8f75f9e7b122ac0f253691a713e</td>
<td>159744</td>
<td>6.132771655252</td>
</tr>
<tr>
<td>.data</td>
<td>4dfa17c08e6128d4db9cea10b5a3d7</td>
<td>77824</td>
<td>4.54069669695</td>
</tr>
</tbody>
</table>

**Packers**

- Name: Microsoft Visual C++ v6.0
- Version: NA
- Entry Point: NA

**Description**

This artifact is a malicious PE32 executable that allows a remote operator or a server to perform various remote operations. When executed, the malware binds to the victim system and listens to activity on port 110. Static analysis indicates the malware's primary purpose is to force a previously compromised server to function as a proxy server. This file is similar in design and functionality to the file C74E289AD927E81D2A1A56BC73E394AB.

**0137F688436C468D43B3E50878EC1A1F**

**Details**

<table>
<thead>
<tr>
<th>Name</th>
<th>0137F688436C468D43B3E50878EC1A1F</th>
</tr>
</thead>
<tbody>
<tr>
<td>Size</td>
<td>737280</td>
</tr>
<tr>
<td>Type</td>
<td>PE32 executable (DLL) (GUI) Intel 80386, for MS Windows</td>
</tr>
<tr>
<td>MD5</td>
<td>0137f688436c468d43b3e50878ec1a1f</td>
</tr>
<tr>
<td>SHA1</td>
<td>f4088bca25fd9ee78119458bfb300721266ecbcb</td>
</tr>
<tr>
<td>ssdeep</td>
<td>6144:MMYkRFxwXGv6d6L6G0kyU/CyS9fNe4fDDxCtMOhYr437HimZ508poBBanFq8StJ:VXv6d0JWFd8BCiv48HepV8gdU0z</td>
</tr>
<tr>
<td>Entropy</td>
<td>6.59562883528</td>
</tr>
</tbody>
</table>

**Antivirus**

- F-secure: Gen:Trojan.Heur.LP.Tu4@a9q3yp
- BitDefender: Gen:Trojan.Heur.LP.Tu4@a9q3yp
- Emsisoft: Gen:Trojan.Heur.LP.Tu4@a9q3yp (B)

**PE Information**

- Compiled: 2016-05-20T07:15:22Z

**PE Sections**

<table>
<thead>
<tr>
<th>Name</th>
<th>MD5</th>
<th>Raw Size</th>
<th>Entropy</th>
</tr>
</thead>
<tbody>
<tr>
<td>(header)</td>
<td>e385ce08c1c7b68edfc2150f3682b256</td>
<td>4096</td>
<td>0.771172194608</td>
</tr>
<tr>
<td>.text</td>
<td>fc14f07cf263b0d1c27ac84ff16072e6</td>
<td>462848</td>
<td>6.59870923197</td>
</tr>
<tr>
<td>.rdata</td>
<td>a5166df020ef131f115707cf8e284ce</td>
<td>147456</td>
<td>5.90353775299</td>
</tr>
<tr>
<td>.data</td>
<td>52711c65208ed70fadd30077524f371ed8</td>
<td>77824</td>
<td>4.90723221684</td>
</tr>
<tr>
<td>.rsrc</td>
<td>6200f67a191ff74151bc8e745b7110</td>
<td>4096</td>
<td>0.0</td>
</tr>
<tr>
<td>.reloc</td>
<td>3dfc4d44b2b523659f00d8945225bc60</td>
<td>40960</td>
<td>5.73692004764</td>
</tr>
</tbody>
</table>

**Packers**

- Name: Microsoft Visual C++ 6.0
- Version: NA
- Entry Point: NA

- Name: Microsoft Visual C++ 6.0 DLL (Debug)
- Version: NA
- Entry Point: NA
**Description**

This artifact is a malicious Windows dynamic-link library (DLL) and is similar in design and functionality to the file C74E289AD927E81D2A1A56BC73E394AB. The primary difference is that this file is a Windows DLL instead of a Windows executable.

Static analysis indicates this application uses the OpenSSL library to add an additional layer of encryption over the traffic between the operator and the proxy malware. The malware accepts four bytes of data, used as an argument to the Win32 API, setsockopt. When executed, this proxy binds to the victim system and listens to activity on port 1030.

**114D8DB4843748D79861B49343C8B7CA**

<table>
<thead>
<tr>
<th>Details</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>114D8DB4843748D79861B49343C8B7CA</td>
</tr>
<tr>
<td><strong>Size</strong></td>
<td>159744</td>
</tr>
<tr>
<td><strong>Type</strong></td>
<td>PE32 executable (GUI) Intel 80386, for MS Windows</td>
</tr>
<tr>
<td><strong>MD5</strong></td>
<td>114d8db4843748d79861b49343c8b7ca</td>
</tr>
<tr>
<td><strong>SHA1</strong></td>
<td>bbff28e84766ad27683cc9078d16f0493cbab</td>
</tr>
<tr>
<td><strong>ssdeep</strong></td>
<td>1536:q17RHwAgW3yPEzf77llovuczbJ4YNiDlovuczbJ4YNi:trNs23t2oPz+n0oPz+nsoPz+n</td>
</tr>
<tr>
<td><strong>Entropy</strong></td>
<td>6.83923058232</td>
</tr>
</tbody>
</table>

**Antivirus**

- **F-secure**: Gen:Variant.Graftor.373993
- **Cyren**: W32/Heuristic-KPPEldorado
- **VirusBlokAda**: BScope.Trojan.Agent
- **BitDefender**: Gen:Variant.Graftor.373993 |
- **Emisoft**: Gen:Variant.Graftor.373993 (B)

**PE Information**

- **Compiled**: 2016-03-01T00:21:03Z

**PE Sections**

<table>
<thead>
<tr>
<th>Name</th>
<th>MD5</th>
<th>Raw Size</th>
<th>Entropy</th>
</tr>
</thead>
<tbody>
<tr>
<td>(.header)</td>
<td>1ce8e90ffa2199ff32be8b977e9a441b</td>
<td>4096</td>
<td>0.65073707439</td>
</tr>
<tr>
<td>.text</td>
<td>caef1f2015675da6b139275b4c7c86d3</td>
<td>40960</td>
<td>6.45414824189</td>
</tr>
<tr>
<td>.rdata</td>
<td>62a4eced0721de04fc52f5fcedf933e44</td>
<td>4096</td>
<td>4.88154271504</td>
</tr>
<tr>
<td>.data</td>
<td>941009d7534325e92b5a0183b05aec00</td>
<td>106496</td>
<td>6.93256592914</td>
</tr>
<tr>
<td>.rsrc</td>
<td>f0a1309490c5ee84dedc04b035c45cd0</td>
<td>4096</td>
<td>0.231410143047</td>
</tr>
</tbody>
</table>

**Packers**

- **Name**: Microsoft Visual C++ v6.0
- **Version**: NA
- **Entry Point**: NA

**Relationships**

(F) 114D8DB4843748D79861B49343C8B7CA (114d8) Characterized_By (S) Figure 1: Hidden Cobra communication flow

**Description**

This artifact is a malicious PE32 executable that allows a remote operator or a server to perform various remote operations. When executed, the malware binds to the victim system and listens to port 1058. Static analysis of this application indicates that its primary purpose is to force a compromised server to function as a proxy server for Internet connections.

This file is similar in design and functionality to the file C74E289AD927E81D2A1A56BC73E394AB, but with the additional capability of providing what appear to be proxied SSL encrypted sessions using public certificates from well-known, legitimate internet services. When communicating with its C2, the malware attempts to disguise traffic by generating a false TLS handshake using a public certificate from one of the sites listed below. Note: the malware does not communicate with any of the servers listed:

--Begin Public Websites--

- myservice.xbox.com
- uk.yahoo.com
- web.whatsapp.com

US-CERT MAR-10135536-B
Static analysis reveals this malware contains an embedded XOR-encoded block of data that is 31,002 bytes in size. The malware decodes this block by XORing it with the value "9Ah". Analysis of this decoded block indicates it contains public SSL encryption certificates for the sites listed above. Strings of interest from the decoded data are displayed below:

--Strings of Interest--

cm1
microsoft1
corp1
redmond1
MSIT Machine Auth CA 20
130322100818Z
150322100818Z0
myservice.xbox.com0
Ohttp://mscrl.microsoft.com/pki/mscorp/crl/MSIT%20Machine%20Auth%20CA%202(1).crl
Mhttps://crl.microsoft.com/pki/mscorp/crl/MSIT%20Machine%20Auth%20CA%202(1).crl
8http://corppki/crl/MSIT%20Machine%20Auth%20CA%202(1).crl0
Ihttp://www.microsoft.com/pki/mscorp/MSIT%20Machine%20Auth%20CA%202(1).crt0D
8http://corppki/aia/MSIT%20Machine%20Auth%20CA%202(1).crt0?

VeriSign, Inc.1
VeriSign Trust Network1:09
2Terms of use at https://www.verisign.com/rpa (c)101/0-
&VeriSign Class 3 Secure Server CA - G30
140924000000Z
150925235959Z0
US1
California1
Sunnyvale1
Yahoo Inc.1
Information Technology1
www.yahoo.com0
DigiCert Inc10%
DigiCert SHA2 Secure Server CA0
130802000000Z
16080512000020I1
US1
California1
Santa Clara1
WhatsApp, Inc.1
web.whatsapp.com0
_xC,aa
gu(
_.mz%`
WpGUUXI
&9Ps
web.whatsapp.com
w1.web.whatsapp.com
This malware uses a cipher and authentication method similar to that used by C74E289AD927E81D2A1A56BC73E394AB for encrypting network communication between itself and a remote operator.

The cipher and communication method, coupled with the malware's ability to create falsified TLS handshake traffic, allows the operator to disguise network connections and obfuscate network traffic sent to and from a remote system.

See Figure 1 below for an illustration of the malware's communication flow using this proxy software.

**Screenshots**

- **Figure 1: Hidden Cobra communication flow**

---

**Details**

<table>
<thead>
<tr>
<th>Name</th>
<th>9E4D9EDB07C348B10863D89B6BB08141</th>
</tr>
</thead>
<tbody>
<tr>
<td>Size</td>
<td>114688</td>
</tr>
<tr>
<td>Type</td>
<td>PE32 executable (DLL) (GUI) Intel 80386, for MS Windows</td>
</tr>
<tr>
<td>MD5</td>
<td>9e4d9edb07c348b10863d89b6bb08141</td>
</tr>
<tr>
<td>SHA1</td>
<td>65122e5129cf74d6b5ebafcc3376aba0145bc14</td>
</tr>
<tr>
<td>ssdeep</td>
<td>1536:fw00XhTH/oB3ALcqmr3+vycketJlovuczcb4YNlS:v6Z1VC3+vycketeoPz+nS</td>
</tr>
<tr>
<td>Entropy</td>
<td>6.05304069999</td>
</tr>
</tbody>
</table>

**Antivirus**
This artifact is a malicious Windows DLL and is similar in design and functionality to the file 114D8DB4843748D79861B49343C8B7CA. The malware also contains 31,002 bytes of XOR-encoded public SSL certificates for public Internet service providers. The public SSL certificates stored within this application are identical to those stored within 114D8DB4843748D79861B49343C8B7CA. It decodes the public SSL certificates via an XOR with the value "9Ah".

### 2950E3741D7AF69E0CA0C5013ABC4209

**Details**

<table>
<thead>
<tr>
<th>Name</th>
<th>2950E3741D7AF69E0CA0C5013ABC4209</th>
</tr>
</thead>
<tbody>
<tr>
<td>Size</td>
<td>827904</td>
</tr>
<tr>
<td>Type</td>
<td>PE32 executable (DLL) (GUI) Intel 80386, for MS Windows</td>
</tr>
<tr>
<td>MD5</td>
<td>2950e3741d7af69e0ca0c5013abc4209</td>
</tr>
<tr>
<td>SHA1</td>
<td>af9db3ed2605572e9897d7106380873045be47b</td>
</tr>
<tr>
<td>ssdeep</td>
<td>12288:Aq/TlttbCSvbcEk8NJ7Wlf/sI5xscSZ/pbEzF87mc+BFHfLMBmLiBpyovNh2M4Ks:Aq7IttbE8JHy87D+9FtMmpyRKWF</td>
</tr>
<tr>
<td>Entropy</td>
<td>6.7996035183</td>
</tr>
</tbody>
</table>

**Antivirus**

- F-secure: Trojan.Inject.RO
- VirusBlokAda: BScope.Trojan.Agent
- Ahnlab: Trojan/Win32.Akdoor

**PE Information**

| Compiled      | 2016-06-22T04:13:36Z |

**PE Sections**

<table>
<thead>
<tr>
<th>Name</th>
<th>MD5</th>
<th>Raw Size</th>
<th>Entropy</th>
</tr>
</thead>
<tbody>
<tr>
<td>(header)</td>
<td>cfc3f97af184f52c091a175eda4587b8</td>
<td>1024</td>
<td>2.71795432504</td>
</tr>
<tr>
<td>.text</td>
<td>51e2667d68017283e27eb2950932c58</td>
<td>539648</td>
<td>6.70314771616</td>
</tr>
<tr>
<td>.rdata</td>
<td>156e8bd71ae9401600f50c1f37e66</td>
<td>175104</td>
<td>6.18962071273</td>
</tr>
<tr>
<td>.data</td>
<td>aa336ce2dce0214bf5fe1d4193d6e99b</td>
<td>66560</td>
<td>5.25915313943</td>
</tr>
<tr>
<td>.rsrc</td>
<td>f77d3025527d2d02be5725f791d038d3</td>
<td>1024</td>
<td>4.79504070454</td>
</tr>
<tr>
<td>.reloc</td>
<td>ceb5df2b67157dbbc6b6aac93c8524f3d</td>
<td>44544</td>
<td>5.79343910767</td>
</tr>
</tbody>
</table>

**Packers**

<table>
<thead>
<tr>
<th>Name</th>
<th>Version</th>
<th>Entry Point</th>
</tr>
</thead>
<tbody>
<tr>
<td>ceb5df2b67157dbbc6b6aac93c8524f3d</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**Description**

The artifact is a malicious Windows DLL application and was identified as a RAT, disguised as an installer for a generic security application. When the file installs, the malware will expect the "SYSTEM\CurrentControlSet\Control\LSA = Security Packages" registry key to be configured properly before loading the DLL onto the operating system as a security package. Analysis suggests an external loader application was used to load this DLL.

The malware searches the system for configuration data by checking for the presence of the registry key "SOFTWARE\Microsoft\Qnuimh = DataPath". If the registry key is not found, the malware attempts to read a file named "system32\msncf.dat" to access the configuration data. If neither the registry key or .dat file are found, the malware's main thread does not execute.

Static analysis of the main thread reveals it is designed to provide C2 of the infected system to a remote operator. This file uses a cipher and authentication method similar to that of files C74E289AD927E81D2A1A56BC73E394AB and 114D8DB4843748D79861B49343C8B7CA.

The malware uses the OpenSSL library to provide an additional layer of SSL encryption to the communications between the operator and malware. This SSL encryption is used in addition to the cipher. The RAT provides the ability to exfiltrate and upload files to and from the compromised system and terminate processes. It also provides the ability to upload and execute secondary payloads. The OpenSSL library and XOR cipher will protect the data uploaded and exfiltrated by the RAT. No hard coded C2s were found in the DLL. However, a common Domain Generation Algorithm was identified, indicating the malware dynamically generates a domain from the current date and time.

---

**964B291AD9B7B4A71DA3F80FB262DBE7**

**Details**

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Size</td>
<td>95232</td>
</tr>
<tr>
<td>Type</td>
<td>PE32+ executable (DLL) (GUI) x86-64, for MS Windows</td>
</tr>
<tr>
<td>MD5</td>
<td>964b291ad9bafa471da3f80fb262db7e</td>
</tr>
<tr>
<td>SHA1</td>
<td>350778fc552918ddd94ea3a956e999990e605</td>
</tr>
<tr>
<td>ssdeep</td>
<td>1536:wMfUQwrWeClpgfAkbU/cnIlytNvMv5K9gnaCrq+gNwv1hqBgLKeTNjw2pS9:wMsQLip6bU/cn7e49ICrq/pwOBgOle8</td>
</tr>
<tr>
<td>Entropy</td>
<td>6.1068715126</td>
</tr>
</tbody>
</table>

**Antivirus**

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>nProtect</td>
<td>Trojan/W64.Agent.95232</td>
</tr>
<tr>
<td>McAfee</td>
<td>Trojan-FLDA/964B291AD9BA</td>
</tr>
<tr>
<td>ClamAV</td>
<td>Win.Trojan.Agent-6319549-0</td>
</tr>
<tr>
<td>Ahnlab</td>
<td>Trojan/Win64.Dllbot</td>
</tr>
<tr>
<td>Quick Heal</td>
<td>Trojan.Generic</td>
</tr>
</tbody>
</table>

**PE Information**

| Compiled   | 2014-03-04T09:43:53Z       |

**PE Sections**

<table>
<thead>
<tr>
<th>Name</th>
<th>MD5</th>
<th>Raw Size</th>
<th>Entropy</th>
</tr>
</thead>
<tbody>
<tr>
<td>(header)</td>
<td>ab32b3c6d7265e57e0829dc1f046728a</td>
<td>1024</td>
<td>2.72686979002</td>
</tr>
<tr>
<td>.text</td>
<td>4aeef9d49dc3f6eaafa76cecb93904875c0</td>
<td>65024</td>
<td>6.26878660906</td>
</tr>
<tr>
<td>.data</td>
<td>7202fd596b05f2d6da7864337a3e3a</td>
<td>15360</td>
<td>5.47919921082</td>
</tr>
<tr>
<td>.data</td>
<td>03ebf79f36469940fda790387d7c1</td>
<td>8192</td>
<td>4.15642395322</td>
</tr>
<tr>
<td>.pdata</td>
<td>324652d914c29afa7a7081d418add47dc</td>
<td>3584</td>
<td>4.7028678328</td>
</tr>
<tr>
<td>.rsrc</td>
<td>f5391c0ba86c6a4b4b4d4b6b6</td>
<td>1536</td>
<td>4.3960032665</td>
</tr>
<tr>
<td>.reloc</td>
<td>2de998d058c83ca559b6a4b4b4d4b6</td>
<td>512</td>
<td>1.93486789339</td>
</tr>
</tbody>
</table>

**Description**

This artifact is a malicious 64-bit DLL. This DLL was installed as a service, with an export "ServiceMain". The installer for this file was not included in the submission. This file contains obfuscated API names and is designed to listen for commands and access requests from a remote server.

When executed, the malware verifies if it is running as a service and attempts to read the following files:

--Begin files--
"%system32%\msncf.dat"
"%AppData%\Local\Temp\~DFB3090EB172633EA.TMP"

--End files--

The files were not part of the submission.

The malware is designed to load or write data into the following registry key:

--Begin key--

hKey = HKEY_LOCAL_MACHINE
Subkey = "SOFTWARE\Microsoft\Pniumj"
ValueName = "DataPath"

--End key--

The data the malware attempts to load or write was not included in the submission.

The malware is designed to listen for commands or access requests from a remote server. This backdoor allows for the following remote operations:

--Begin operations--

Mimic Timestamp
Execute Shell Command
Change Listening Port and proxy
Gather system information
Upload files Install configuration in the registry
Create, start, and terminate a new process and its primary thread
Search, read, write, move, download, and execute files
Delete all artifacts associated with the malware from the infected system
Send Status
Retrieves information about all installed disk, including the disk type and the amount of free space on the disk

--End operations--

Relationship Summary

(F) 114D8DB4843748D79861B49343C8B7CA Characterized_By (S) Figure 1: Hidden Cobra communication flow Characterizes (F) 114D8DB4843748D79861B49343C8B7CA

(S) Figure 1: Hidden Cobra communication flow

Mitigation Recommendations

US-CERT would like to remind users and administrators of the following best practices to strengthen the security posture of their organization's systems:

- Maintain up-to-date antivirus signatures and engines.
- Restrict users' ability (permissions) to install and run unwanted software applications.
- Enforce a strong password policy and implement regular password changes.
- Exercise caution when opening e-mail attachments even if the attachment is expected and the sender appears to be known.
- Keep operating system patches up-to-date.
- Enable a personal firewall on agency workstations.
- Disable unnecessary services on agency workstations and servers.
- Scan for and remove suspicious e-mail attachments; ensure the scanned attachment is its "true file type" (i.e., the extension matches the file header).
- Monitor users' web browsing habits; restrict access to sites with unfavorable content.
- Exercise caution when using removable media (e.g., USB thumbdrives, external drives, CDs, etc.).
- Scan all software downloaded from the Internet prior to executing.
- Maintain situational awareness of the latest threats; implement appropriate ACLs.
### Contact Information

- 1-888-282-0870
- [soc@us-cert.gov](mailto:soc@us-cert.gov) (UNCLASS)
- [us-cert@dhs.sgov.gov](mailto:us-cert@dhs.sgov.gov) (SIPRNET)
- [us-cert@dhs.ic.gov](mailto:us-cert@dhs.ic.gov) (JWICS)

US-CERT continuously strives to improve its products and services. You can help by answering a very short series of questions about this product at the following URL: [https://forms.us-cert.gov/ncsd-feedback/](https://forms.us-cert.gov/ncsd-feedback/)

### Document FAQ

**What is a MAR?** A Malware Analysis Report (MAR) is intended to provide detailed code analysis and insight into specific tactics, techniques, and procedures (TTPs) observed in the malware.

**Can I edit this document?** This document is not to be edited in any way by recipients. All comments or questions related to this document should be directed to the US-CERT Security Operations Center at 1-888-282-0870 or [soc@us-cert.gov](mailto:soc@us-cert.gov).

**Can I submit malware to US-CERT?** Malware samples can be submitted via three methods. Contact us with any questions.
- Web: [https://malware.us-cert.gov](https://malware.us-cert.gov)
- E-Mail: [submit@malware.us-cert.gov](mailto:submit@malware.us-cert.gov)
- FTP: ftp.malware.us-cert.gov/malware (anonymous)

US-CERT encourages you to report any suspicious activity, including cybersecurity incidents, possible malicious code, software vulnerabilities, and phishing-related scams. Reporting forms can be found on US-CERT's homepage at [www.us-cert.gov](http://www.us-cert.gov).