Advisory: APT29 targets COVID-19 vaccine development

Version 1.1
16 July 2020
© Crown Copyright 2020
About this document

This report details recent Tactics, Techniques and Procedures (TTPs) of the group commonly known as ‘APT29’, also known as ‘the Dukes’ or ‘Cozy Bear’.

This report provides indicators of compromise as well as detection and mitigation advice.

Disclaimer

This report draws on information derived from multiple sources. Any NCSC findings and recommendations made have not been provided with the intention of avoiding all risks, and following the recommendations will not remove all such risk. Ownership of information risks remains with the relevant system owner at all times.
Introduction

The United Kingdom’s National Cyber Security Centre (NCSC) and Canada’s Communications Security Establishment (CSE) assess that APT29 (also known as ‘the Dukes’ or ‘Cozy Bear’) is a cyber espionage group, almost certainly part of the Russian intelligence services. The United States’ National Security Agency (NSA) agrees with this attribution and the details provided in this report.

The United States’ Department of Homeland Security’s Cybersecurity and Infrastructure Security Agency (DHS CISA) endorses the technical detail and mitigation advice provided in this advisory.

The group uses a variety of tools and techniques to predominantly target governmental, diplomatic, think-tank, healthcare and energy targets for intelligence gain.

Throughout 2020, APT29 has targeted various organisations involved in COVID-19 vaccine development in Canada, the United States and the United Kingdom, highly likely with the intention of stealing information and intellectual property relating to the development and testing of COVID-19 vaccines.

APT29 is using custom malware known as ‘WellMess’ and ‘WellMail’ to target a number of organisations globally. This includes those organisations involved with COVID-19 vaccine development. WellMess and WellMail have not previously been publicly associated to APT29.

Details of techniques

Initial infection vectors

The group frequently uses publicly available exploits to conduct widespread scanning and exploitation against vulnerable systems, likely in an effort to obtain authentication credentials to allow further access. This broad targeting potentially gives the group access to a large number of systems globally, many of which are unlikely to be of immediate intelligence value. The group may maintain a store of stolen credentials in order to access these systems in the event that they become more relevant to their requirements in the future.

In recent attacks targeting COVID-19 vaccine research and development, the group conducted basic vulnerability scanning against specific external IP addresses owned by the organisations. The group then deployed public exploits against the vulnerable services identified.
The group has been successful using recently published exploits to gain initial footholds. Examples include, but are not limited to:

- **CVE-2019-19781 Citrix** [1]
- **CVE-2019-11510 Pulse Secure** [2]
- **CVE-2018-13379 FortiGate** [2]
- **CVE-2019-9670 Zimbra** [3]

The group likely seeks to take full advantage of a variety of new exploits when publicised. More information about these exploits can be found in previous NCSC advisories on [Citrix](https://www.citrix.com) and [VPN vulnerabilities](https://www.cisco.com) [1,2].

The group also uses spear-phishing to obtain authentication credentials to internet-accessible login pages for target organisations.

**Persistent access**

Upon gaining access to a system, the group likely drops further tooling and/or seeks to obtain legitimate credentials to the compromised systems in order to maintain persistent access. The actor is likely to use anonymising services when using the stolen credentials.

**WellMess malware**

In some cases, APT29 also deploys custom malware known as WellMess or WellMail to conduct further operations on the victim’s system.

WellMess is malware written in either Golang or .NET and has been in use since at least 2018. WellMess was first reported on by [JPCERT](https://www.jpcert.or.jp) and [LAC](https://www.lac.co.jp) researchers in July 2018[4][5]. It is named after one of the function names in the malware - ‘wellmess’. WellMess is a lightweight malware designed to execute arbitrary shell commands, upload and download files. The malware supports HTTP, TLS and DNS communications methods.

Indicators of compromise (IOCs) for WellMess are available in the [appendix](#).

**WellMail malware**

WellMail is a lightweight tool designed to run commands or scripts with the results being sent to a hardcoded Command and Control (C2) server.

The NCSC has named this malware ‘WellMail’ due to file paths containing the word ‘mail’ and the use of server port 25 present in the sample analysed. Similar to WellMess, WellMail uses hard-coded client and certificate authority TLS certificates to communicate with C2 servers.
The binary is an ELF utility written in Golang which receives a command or script to be run through the Linux shell. To our knowledge, WellMail has not been previously named in the public domain.

IOCs for WellMail are available in the appendix.

Certificate usage

WellMess and WellMail samples contained TLS certificates with the hard-coded subjectKeyIdentifier (SKI) '0102030406', and used the subjects 'C=Tunis, O=IT' and 'O=GMO GlobalSign, Inc' respectively. These certificates can be used to identify further malware samples and infrastructure. Servers with this GlobalSign certificate subject may be used for other functions in addition to WellMail malware communications.

SoreFang malware

Malware, dubbed 'SoreFang' by the NCSC, is a first stage downloader that uses HTTP to exfiltrate victim information and download second stage malware. The sample analysed by the NCSC contains the same infrastructure as a WellMess sample (103.216.221[.]19).

It is likely that SoreFang targets SangFor devices. Industry reporting indicates that other actors, reportedly including 'DarkHotel', have also targeted SangFor devices. Therefore, not all SangFor exploitation activity relates to targeting by APT29.

Conclusion

APT29 is likely to continue to target organisations involved in COVID-19 vaccine research and development, as they seek to answer additional intelligence questions relating to the pandemic.

It is strongly recommended that organisations use the rules and IOCs in the appendix in order to detect the activity detailed in this advisory.
## Appendix

### Indicators of compromise and detection rules

#### WellMess IOCs

<table>
<thead>
<tr>
<th>Hashes</th>
</tr>
</thead>
<tbody>
<tr>
<td>00654dd07721e7551641f90c8ba38e98c0aca0b30e2848e5efc0e1752c067ec07</td>
</tr>
<tr>
<td>0322c4c2d51f173ab55bf3f43b1b0f152188d7146cc67ff497ad2759d3dd1c20f</td>
</tr>
<tr>
<td>03e9adaed52955961f1f18212ff70181b3de0e3da3d7f22961a6221c9da2dd2e</td>
</tr>
<tr>
<td>0b8e6a1llda3dfdf120ec15846bb966d6747d24bb92e3e43d63b665e0698e0193</td>
</tr>
<tr>
<td>14e9b5e214572c3b13ff8772d680633f5e2e38259043357c943026545c46cadd2</td>
</tr>
<tr>
<td>1fed2e1bb077af08d7fbb5eccf22e5169d5289a825dcafe2d8742b0b030e487641</td>
</tr>
<tr>
<td>21129ad1780b011cd3b6906a7d6f105e3bdc1f445757f77df58ba9164b0a0c9b9</td>
</tr>
<tr>
<td>2285a264ffab9a5b1e6b4e2b9bcab9baf26750bc6551ee03094af56a444ac41</td>
</tr>
<tr>
<td>2daba46f950cd5b77481e605a5ee0f28bf14cedfcd8e4361935e5045c23bc38</td>
</tr>
<tr>
<td>49bbff6b91ee71bbdf8fd94829391a36b844ffba104c14e501c92732ada528b</td>
</tr>
<tr>
<td>4c8671411da91eb596f408c2a6ff66a25f7c40c65ff4e333b352a711bf9c</td>
</tr>
<tr>
<td>5ca4a9f6553fe66ad2c7244bf7d0fac2b372f9e7c2e200814c98ac467172fb</td>
</tr>
<tr>
<td>797159c202ca413566ee18c5303d37e9d2a43ca43d0ce02e1fd9e7045b925d1</td>
</tr>
<tr>
<td>7c39841ba409bce4c2c35437ec043f229109f84325c70b9530edf15d826147ee</td>
</tr>
<tr>
<td>84b846a42d9431520d3d214262f3d3a5d9676eb560aa7e471b853d1630ca403</td>
</tr>
<tr>
<td>8749c1495af4f4d73ccfcf84b32f556e57b8549df81eefeb01c1dc3475a7434568a</td>
</tr>
<tr>
<td>92a856a2261e10749bee086e1clce8cfe1e14151457a24753915fd375e5a188b4d9</td>
</tr>
<tr>
<td>9e39838ae8a2371d4579c4e1035157d887a84bbfe66fbb3769c5637d59c75</td>
</tr>
<tr>
<td>953b5f9927e2d50f3f72c6ec85e894293717830c0ed6d468e2933a7e99a</td>
</tr>
<tr>
<td>a03a71765b1b0e07e4e4fbcb557dca995f9068e92db9b2dada9dd084203145</td>
</tr>
<tr>
<td>a17b2a904c24df62581500176183fbc202a7404e4f1976cdcf01e664a20292</td>
</tr>
<tr>
<td>a3ca4e1e083b93ea90ace1ca30d9ef71163e8a95ee00500cb3df021ada1c8a</td>
</tr>
<tr>
<td>b7f5a5be703d9ba3721d046db80f62886e10009b45fa5cddf73ce7f89ff53e5a</td>
</tr>
<tr>
<td>bec1981e42c1e01c145113d84a33c9bccc66456c1274bbac073da82a5f537d</td>
</tr>
<tr>
<td>c1a0b73bad4ca30a5c15db56c1cbaf45f5b75f3d53dcaf62ddc598aee2933453f</td>
</tr>
<tr>
<td>d7e1782f484094f5c83f5f0e82ad2d8544530ebd3a9051d2205b73040381</td>
</tr>
<tr>
<td>dd3a0c596fd699900cd1003f097e6614ac69787edfa6fa84a8f471ecb836bb</td>
</tr>
<tr>
<td>e3296073990a1483f3f1447e002653a5a8ad8d65ff77fbd2c5a841a90aaf0f</td>
</tr>
<tr>
<td>e3d605b4c2a7d8fa7250f0781ea6dab4a977551c13fe2f9a86f3519b2ae9a</td>
</tr>
<tr>
<td>f3af3949d93c6fbdf50b647304c0a591a1a43d56361e6c0f1c2f332a702ad</td>
</tr>
<tr>
<td>f622d031207d22c633ccce187a24c50980243cb4717d21fad6588dcbefc929e9</td>
</tr>
<tr>
<td>f3969d32398bbee3709e9da5f83269535de664bcb36753bd41a0b11172c950</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IP Addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>103.103.128[..]221</td>
</tr>
<tr>
<td>103.13.240[..]46</td>
</tr>
<tr>
<td>103.205.8[..]72</td>
</tr>
<tr>
<td>103.216.221[..]19</td>
</tr>
<tr>
<td>103.253.41[..]102</td>
</tr>
<tr>
<td>103.253.41[..]68</td>
</tr>
<tr>
<td>103.253.41[..]182</td>
</tr>
<tr>
<td>103.253.41[..]90</td>
</tr>
<tr>
<td>103.73.188[..]101</td>
</tr>
<tr>
<td>111.90.146[..]143</td>
</tr>
<tr>
<td>111.90.150[..]176</td>
</tr>
<tr>
<td>119.160.234[..]163</td>
</tr>
<tr>
<td>119.160.234[..]194</td>
</tr>
<tr>
<td>119.81.173[..]130</td>
</tr>
<tr>
<td>119.81.178[..]105</td>
</tr>
<tr>
<td>120.53.12[..]132</td>
</tr>
</tbody>
</table>
Yara Rules

rule wellmess_dotnet_unique_strings {
    meta:
        description = "Rule to detect WellMess .NET samples based on unique strings and function/variable names"
        author = "NCSC"
        hash = "2285a264ffab59ab5a1eb4e2b9bcab9baf26750b6c551ee3094af56a4442ac41"
    strings:
        $s1 = "MaxPostSize" wide
        $s2 = "HealthInterval" wide
        $s3 = "Hello from Proxy" wide
        $s4 = "Start bot:" wide
        $s5 = "Choise" ascii wide
        $s7 = "FromNormalToBase64" ascii
        $s8 = "FromBase64ToNormal" ascii
        $s9 = "ConvBytesToWords" ascii
        $s10 = "WellMess" ascii
        $s11 = "chunksM" ascii
    condition:
        uint16(0) == 0x5a4d and uint16(uint16(0x3c)) == 0x4550 and 3 of them
}

rule wellmess_botlib_function_names {
description = "Rule to detect WellMess Golang samples based on the function names used by the actor"
author = "NCSC"
hash = "8749c1495af4fd73ccfc84b32f56f5e78549d81feefb0c1d1c3475a74345f6a8"
strings:
  $s1 = "botlib.wellMess" ascii wide
  $s2 = "botlib.saveFile" ascii wide
  $s3 = "botlib.reply" ascii wide
  $s4 = "botlib.init" ascii wide
  $s5 = "botlib.generateRandomString" ascii wide
  $s6 = "botlib.encrypt" ascii wide
  $s7 = "botlib.deleteFile" ascii wide
  $s8 = "botlib.convertFromString" ascii wide
  $s9 = "botlib.chunksM" ascii wide
  $s10 = "botlib.Work" ascii wide
  $s11 = "botlib.UnpackB" ascii wide
  $s12 = "botlib.Unpack" ascii wide
  $s13 = "botlib.UDFFile" ascii wide
  $s14 = "botlib.Split" ascii wide
  $s15 = "botlib.Service" ascii wide
  $s16 = "botlib.SendMessage" ascii wide
  $s17 = "botlib.Send.func1" ascii wide
  $s18 = "botlib.Send" ascii wide
  $s19 = "botlib.ReceiveMessage" ascii wide
  $s20 = "botlib.RandStringBytes" ascii wide
  $s21 = "botlib.RandInt" ascii wide
  $s22 = "botlib.Post" ascii wide
  $s23 = "botlib.Parse" ascii wide
  $s24 = "botlib.Pad" ascii wide
  $s25 = "botlib.Pack" ascii wide
  $s26 = "botlib.New" ascii wide
  $s27 = "botlib.KeySizeError.Error" ascii wide
  $s28 = "botlib.Key" ascii wide
  $s29 = "botlib.Join" ascii wide
  $s30 = "botlib.GetRandomBytes" ascii wide
  $s31 = "botlib.GenerateSymmKey" ascii wide
  $s32 = "botlib.FromNormalToBase64" ascii wide
  $s33 = "botlib.EncryptText" ascii wide
  $s34 = "botlib.Download" ascii wide
  $s35 = "botlib.Decipher" ascii wide
  $s36 = "botlib.Command" ascii wide
  $s37 = "botlib.Cipher" ascii wide
  $s38 = "botlib.CalculateMD5Hash" ascii wide
  $s39 = "botlib.Base64ToNormal" ascii wide
  $s40 = "botlib.AES_Encrypt" ascii wide
  $s41 = "botlib.AES_Decrypt" ascii wide
  $s42 = "botlib.(*rc6cipher).Encrypt" ascii wide
  $s43 = "botlib.(*rc6cipher).Decrypt" ascii wide
  $s44 = "botlib.(*rc6cipher).BlockSize" ascii wide
  $s45 = "botlib.(*KeySizeError).Error" ascii wide
  $s46 = "botlib.DownloadDNS" ascii wide
  $s47 = "botlib.JoinDnsChunks" ascii wide
  $s48 = "botlib.SendDNS" ascii wide
  $s49 = "botlib.CreateDNSName" ascii wide
condition:
  ((uint16(0) == 0x5a4d and uint16(uint16(0x3c)) == 0x4550) or uint32(0) == 0x464c457f) and any of them
rule wellmess_certificate_base64_snippets {
  meta:
    description = "Rule for detection of WellMess based on base64 snippets of certificates used"
    author = "NCSC"
    hash = "8749c1495af4fd73ccfc84b32f56f5e78549d81feefb0c1d1c3475a74345f6a8"
  strings:
    $a1 = "BgNVHQ4EBwQFAQIDBA"
    $a2 = "YDVQ0OBAcEBQECAwQG"
    $a3 = "GA1UDgQHBAUAQMEB"
    $b1 = "BgNVBAYTBVR1bm1zMQswCQYDVQQKEwJJVD"
    $b2 = "YDVQQGEwVUdW5pczElMAkGA1UEChMCSVQx"
    $b3 = "GA1UEBhMFVHVuaXMxMzAJBgNVBAoTAK1UM"
  condition:
    ((uint16(0) == 0x5a4d and uint16(uint16(0x3c)) == 0x4550) or uint32(0) == 0x464c457f) and any of ($a*) and any of ($b*)
}

rule wellmess_regex_used_for_parsing_beacons {
  meta:
    description = "Detects WellMess Golang and .NET samples based on the regex they used to parse commands and beacon information"
    author = "NCSC"
    hash = "8749c1495af4fd73ccfc84b32f56f5e78549d81feefb0c1d1c3475a74345f6a8"
  strings:
    $a = "fileName: (?<fn>.*?)\\sargs: (?<arg>.*?)\\snotwait: (?<nw>.*?)"
    $b = "<; (?<key>[^<]*?)>; (?<value>[^<]*?)<[^>]*?>; " ascii wide
  condition:
    ((uint16(0) == 0x5a4d and uint16(uint16(0x3c)) == 0x4550) or uint32(0) == 0x464c457f) and any of them
}

WellMail IOCs

<table>
<thead>
<tr>
<th>Hashes</th>
</tr>
</thead>
<tbody>
<tr>
<td>83014ab5b3f63b0253cdab6d715f5988ac9014570fa4ab2b267c7cf9ba237d18 (UPX)</td>
</tr>
<tr>
<td>0c5ad1e8fe43583e279201cdb1046aa742bae59685e6da24e963a41df987494 (Unpacked)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IP Addresses (Malware)</th>
</tr>
</thead>
<tbody>
<tr>
<td>103.216.221[].19</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IP Addresses (‘GlobalSign’ certificate, operated by APT29 but not necessarily used for WellMail malware communications)</th>
</tr>
</thead>
<tbody>
<tr>
<td>119.81.184[].11</td>
</tr>
<tr>
<td>185.225.226[].16</td>
</tr>
<tr>
<td>188.241.68[].137</td>
</tr>
<tr>
<td>45.129.229[].48</td>
</tr>
</tbody>
</table>
**Yara Rules**

```yara
rule wellmail_unique_strings {
  meta:
    description = "Rule for detection of WellMail based on unique strings contained in the binary"
    author = "NCSC"
    hash = "0c5ad1e8fe43583e279201cdb1046aea742bae59685e6da24e963a41df987494"
  strings:
    $a = "C:\Server\Mail\App_Data\Temp\agent.sh\src"
    $b = "C:/Server/Mail/App_Data/Temp/agent.sh/src/main.go"
    $c = "HgQdbx4qRNv"
    $d = "042a51567eea19d5aca71050b4535d33d2ed43ba"
    $e = "main.zipit"
    $f = "@[^s]+?s(?P<tar>.*)s"
  condition:
    uint32(0) == 0x464C457F and 3 of the
}
```

```yara
rule wellmail_certificate_base64_snippets {
  meta:
    description = "Rule for detection of WellMail based on base64 snippets of certificates used"
    author = "NCSC"
    hash = "0c5ad1e8fe43583e279201cdb1046aea742bae59685e6da24e963a41df987494"
  strings:
    $a1 = "BgNVHQ4EBwQFAQIDBA"
    $a2 = "YDVR0OBAcEBQECAwQG"
    $a3 = "GA1UdDgQHBAUBAgMEB"
    $b1 = "BgNVBAoTE0dNTyBHbG9iYWxTaWduLCBJbm"n
    $b2 = "YDVQQKExNHTU8gR2xvYmFsU2lnbiwgSW5j"
    $b3 = "GA1UEChMT R01PIEdsb2JhbFNpZ24sIEluY"
  condition:
    uint32(0) == 0x464C457F and any of ($a*) and any of ($b*)
}
```

**SoreFang IOCs**

**Hashes**

<table>
<thead>
<tr>
<th>Hash</th>
</tr>
</thead>
<tbody>
<tr>
<td>58d8e65976b53b77645c248bfa18c3b87a6ecfb02f306fe6ba4944db96a5ede2</td>
</tr>
<tr>
<td>65495d173e305625696051944a36a031ea94bb3a4f13034d8be740982bc4ab75</td>
</tr>
<tr>
<td>a4b790ddff3d2e6691dcacae08fb0bfalae56b6c73d70688b097f8a31af064</td>
</tr>
</tbody>
</table>

**IP Addresses (Malware)**

<table>
<thead>
<tr>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>103.216.221[.]19</td>
</tr>
</tbody>
</table>

**Yara Rules**

```yara
rule sorefang_directory Enumeration_output_strings {
  meta:
    description = "Rule to detect SoreFang based on formatted string output for directory enumeration"
    author = "NCSC"
    hash = "58d8e65976b53b77645c248bfa18c3b87a6ecfb02f306fe6ba4944db96a5ede2"
```
strings:
  $ = "----------All usres directory----------"
  $ = "----------Desktop directory----------"
  $ = "----------Documents directory----------"
condition:
  (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and any of
  them
}

rule sorefang_encryption_key_2b62 {
  meta:
    description = "Rule to detect SoreFang based on hardcoded encryption
key"
    author = "NCSC"
    hash = "58d8e65976b53b77645c248bfa18c3b87a6ecfb02f306fe6ba4944db96a5ede2"
  strings:
    $ = "2b6233eb3e872ff78988f4a8f3f6a3ba"
  condition:
    (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and any of
    them
}

rule sorefang_encryption_key_schedule {
  meta:
    description = "Rule to detect SoreFang based on the key schedule used
for encryption"
    author = "NCSC"
    hash = "58d8e65976b53b77645c248bfa18c3b87a6ecfb02f306fe6ba4944db96a5ede2"
  strings:
    $ = {C7 05 ?? ?? ?? ?? 63 51 E1 B7 B8 ?? ?? ?? ?? BB 48 FC 81 E9 47
      86 C8 61 89 08 83 C0 04 3D ?? ?? ?? ?? 7E EB 33 D2 33 33 33 B8 2C 00 00 00
      89 55 3E 33 F6 89 3D 4B 3B 3F 08 4F 4F 7C 3D 0F 1F 80 00 00 00 00}
  condition:
    (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and any of
    them
}

rule sorefang_command_elem_cookie Ga_boundary_string {
  meta:
    description = "Rule to detect SoreFang based on scheduled task
element and Cookie header/boundary strings"
    author = "NCSC"
    hash = "58d8e65976b53b77645c248bfa18c3b87a6ecfb02f306fe6ba4944db96a5ede2"
  strings:
    $ = "<Command>" wide
    $ = "Cookie: ga="
    $ = "----------974767299852498929531610575"
  condition:
    (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and 2 of
    them
}
rule_sorefang_encryption_round_function {
  meta:
    description = "Rule to detect SoreFang based on the encryption round function"
    author = "NCSC"
    hash = "58d8e6597eb53b77645c248bfa18c3b87a6ecfb02f306fe6ba4944db96a5ede2"
  strings:
    $ = {8A E9 8A FB 8A 5D 0F 02 C9 88 45 0F FE C1 0F BE C5 88 6D F3 8D 14 45 01 00 00 00 0F AF D0 0F BE C1 89 55 E4 8D 14 45 01 00 00 00 0F AF D0 8B C1} 
    condition:
      (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and any of them
}

rule_sorefang_add_random_commas_spaces {
  meta:
    description = "Rule to detect SoreFang based on function that adds commas and spaces"
    author = "NCSC"
    hash = "58d8e6597eb53b77645c248bfa18c3b87a6ecfb02f306fe6ba4944db96a5ede2"
  strings:
    $ = {E8 ?? ?? ?? ?? ?? B9 06 00 00 00 99 F7 F9 8B CE 83 FA 04 7E 09 6A 02 6A ?? ?? ?? ?? EB 07 6A 01 68 ?? ?? ?? ?} 
    condition:
      (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and any of them
}

rule_sorefang_modify_alphabet_custom_encode {
  meta:
    description = "Rule to detect SoreFang based on arguments passed into custom encoding algorithm function"
    author = "NCSC"
    hash = "58d8e6597eb53b77645c248bfa18c3b87a6ecfb02f306fe6ba4944db96a5ede2"
  strings:
    $ = {33 C0 8B CE 6A 36 6A 71 66 89 46 60 88 46 62 89 46 68 66 89 46 64} 
    condition:
      (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and any of them
}

rule_sorefang_custom_encode_decode {
  meta:
    description = "Rule to detect SoreFang based on the custom encoding/decoding algorithm function"
    author = "NCSC"
    hash = "58d8e6597eb53b77645c248bfa18c3b87a6ecfb02f306fe6ba4944db96a5ede2"
  strings:
    $ = {55 8B EC 8B D1 53 56 8B 75 08 8B DE 80 42 62 FA 8A 4A 62 66 D3 EB 57 3A 5A 5C 74 0F} 

condition: (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and any of them
}

rule sorefang_remove_chars_comma_space_dot {
  meta:
    description = "Rule to detect SoreFang based on function that removes commas, spaces and dots"
    author = "NCSC"
    hash = "58d8e65976b53b77645c248bfa18c3b87a6ecfb02f306fe6ba4944db96a5ede2"
  strings:
    $ = {8A 18 80 FB 2C 74 03 88 19 41 42 40 3B D6 75 F0 8B 5D 08}
    $ = {8A 18 80 FB 2E 74 03 88 19 41 42 40 3B D6 75 F0 8B 5D 08}
    $ = {8A 18 80 FB 20 74 03 88 19 41 42 40 3B D6 75 F0 8B 5D 08}
  condition:
    (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and all of them
}

rule sorefang_disk Enumeration_strings {
  meta:
    description = "Rule to detect SoreFang based on disk enumeration strings"
    author = "NCSC"
    hash = "a4b790ddff3b32e6691dcaec08fb0bfalae56b6c73d70688b097ffa831af064"
  strings:
    $ = "\x0D\x0AFree on disk: "
    $ = "Total disk: "
    $ = "Error in GetDiskFreeSpaceEx\x0D\x0A"
    $ = "\x0D\x0AVolume label: "
    $ = "Serial number: "
    $ = "File system: "
    $ = "Error in GetVolumeInformation\x0D\x0A"
    $ = "I can not het information about this disk\x0D\x0A"
  condition:
    (uint16(0) == 0x5A4D and uint16(uint32(0x3c)) == 0x4550) and all of them
}
### External Reading


### Mitigation

A variety of mitigations will be of use in defending against the campaigns detailed in this report:

- **Protect your devices and networks by keeping them up to date**: use the latest supported versions, apply security patches promptly, use anti-virus and scan regularly to guard against known malware threats. See NCSC Guidance: [https://www.ncsc.gov.uk/guidance/mitigating-malware](https://www.ncsc.gov.uk/guidance/mitigating-malware).

- **Use multi-factor authentication (2-factor authentication/two-step authentication) to reduce the impact of password compromises.** See NCSC Guidance: [https://www.ncsc.gov.uk/guidance/multi-factor-authentication-online-services](https://www.ncsc.gov.uk/guidance/multi-factor-authentication-online-services) and [https://www.ncsc.gov.uk/guidance/setting-two-factor-authentication-2fa](https://www.ncsc.gov.uk/guidance/setting-two-factor-authentication-2fa)

- **Treat people as your first line of defence.** Tell staff how to report suspected phishing emails, and ensure they feel confident to do so. Investigate their reports promptly and thoroughly. Never punish users for clicking phishing links or opening attachments. See NCSC Guidance: [https://www.ncsc.gov.uk/phishing](https://www.ncsc.gov.uk/phishing)

- **Set up a security monitoring capability** so you are collecting the data that will be needed to analyse network intrusions. See NCSC Guidance: [https://www.ncsc.gov.uk/guidance/introduction-logging-security-purposes](https://www.ncsc.gov.uk/guidance/introduction-logging-security-purposes)

- **Prevent and detect lateral movement in your organisation’s networks.** See NCSC Guidance: [https://www.ncsc.gov.uk/guidance/preventing-lateral-movement](https://www.ncsc.gov.uk/guidance/preventing-lateral-movement)