University Researchers Located in Hong Kong Targeted with Demsty

Version: 1.0 (26.June.2017)

Executive summary

A new OSX backdoor was emailed as an attachment in an spearphishing campaign to multiple University science and business researchers located in Hong Kong at the beginning of June 2017. The sender´s email was another account within the University.

We call this backdoor Demsty.

A previous spearphishing event occurred on May 24th 2017 at the same organization, but this one was detected and removed at the mail server itself. This second June spearphishing campaign is the only event related with this malware we have observed globally, suggesting attacks to date have been highly selective.

The initial deployment for this backdoor goes back to April 2017. Generally speaking, the group behind the attack appears to be interested in stealing intellectual property related to advanced technology in multiple fields and applications. This cluster of activity TTPs reminds us of previous CN-APT activity and resources than suspected WildNeutron.

This paper in a nutshell :

- A not-confirmed-yet APT actor spearphished multiple researchers in Hong Kong with the OSX Demsty backdoor;
- Attackers appear to have assumed the identity of a Hong Kong scientist;
- Demsty spearphishing to date relied on social engineering, and lacks zero-day or half-day exploits.

For more information please contact: intelreports@kaspersky.com

Technical Analysis

To date the actor behind this campaign has not deployed any zero or half-day exploits, and instead relies on social engineering techniques. The tactics in the wave of spearphish in April 2017 appear to have been similar to this later event.

On May 24th, 2017, a malicious emailed object[1] detected with the “HEUR:Backdoor.OSX.Demsty.a” verdict was detected at a Linux mail server at a University in Hong Kong. Despite the detection it appears that the attackers were able to get in. A second spearphishing effort was made from within the University mail system.

The second message was sent on 2017/06/02 17:01:24 with a subject line regarding a private meeting: “Re:Confidential Data about Tomorrows's Meeting for Mac” and a different but similar zip attachment “Confidential_Data.zip”. This second 64-bit mach-O binary[2] exactly matches the 216,370 byte size of the previously observed “Backdoor.OSX.Demsty.a” binary. The message came from one identity within the University. Either the account is compromised, or the University is running an internally open SMTP relay. The mail relay is not exposed to the public internet.

The attackers may have used a contact list from the real account, as they sent this OSX malware to researchers using Windows systems as well.
The researcher the compromised account belongs to is cited publicly in academic Bio-Chemistry articles. Spearphish recipients are located within the same University, so this targeting and activity is highly likely life-science related, possibly related to the development and use of molecular beacons and other advanced tools in biochem experiments run in their lab.

The subject line contains a pretty obvious spelling error regarding “Tomorrows’s” meeting, which a non-native speaker may not notice at send. We also note a mis-spelling in the hardcoded malware strings. The email was sent to at least four other individual accounts within the University. It appears that the email was sent to all recipients at once.

Malware Analysis - Demsty

```
Backdoor shell module
MD5: f0266724ff69e5ab819e554e33d39042
Observed: 2017-06-02 17:01:24
Size: 216,370 bytes
Type: Mac OS X Mach-O 64bit Intel executable

MD5: 7578d23e160073cfac6fd65e426c6504
```

[1] 7578d23e160073cfac6fd65e426c6504

[2] f0266724ff69e5ab819e554e33d39042

```
Observed: 2017-05-24 11:08
Size: 216,370 bytes
Type: Mac OS X Mach-O 64bit Intel executable

MD5: 545aaf30e7f7e1f786257d933b50f2da
Observed: 2017-04-22
Size: 190,554 bytes
Type: Mac OS X Mach-O 64bit Intel executable
```

Demsty is a modular backdoor by design, providing system and user detail collection, cmd shell execution, file and permissions management, update management, 3DES encryption, c2 http communications, and plug-in support capabilities. Configuration data is stored 3DES encrypted. While we haven't collected a Demsty plug-in, we have observed changes in the Demsty backdoor itself, increasing its size from early versions at 187kb to the late May/early June version at 212kb. Finally, the group appears to focus on OSX with this backdoor, as there is no known Windows support or Windows comparable for Demsty.

Persistence

The malware starts by establishing its own persistence through the common method of registering a startup item. It creates a plist file in the following persistence directories:

```
/System/Library/LaunchDaemons/
/Library/LaunchDaemons/
/System/Library/LaunchAgents/
/Library/LaunchAgents/
```

The property list file is created under the name 'com.appple.sysetmd', a misspelling of the legitimate native component systemd.

The plist file points to binaries located in user folders:

```
~/.local/bin/keyboardime
~/.local/bin/sysetmd
```

It then proceeds to fork itself for persistence in memory.

The malware also attempts some autoprotectiong by hiding and locking itself down. It attempts to prevent removal by setting the immutable bit on its files and folders. Doing so prevents even the root account from deleting the filesystem objects:

```
chflags uchg <path>/sysetmd
chflags schg <path>/sysetmd
```

It also attempts to hide itself on the filesystem using the chflags utility:

```
chflags hidden <path>/sysetmd
```

Scattered strings used in various system file creation are obfuscated with a simple xor 'YYYY' algorithm, most likely to evade simple detection schemes:

```
com.appule.sysetmd
/System/Library/StartupItems/
/Library/StartupItems/
/tmp/.systemd/
systemd.lock
system_upgrade
pluginxxx.tmp
/tmp/.kbdr-unix/
kbdime.lock
/.local/bin/keyboardime
/.local/bin/sysetmd
/Library/sysetmd
/Library/keyboardime
ys./pmt/Y/dmets
```

System information is collected by calling and parsing the results of Apple provided system utilities:

```
sysctl -a |grep machdep.cpu.brand_string|cut -d ':' -f2
sysctl -a |grep hw.memsize: |cut -d ':' -f2
```

The backdoor self-identifies, collects, and reports the external IP it is communicating over with a call to one of a handful of "whatismyip" services:

```
whatismyip.akamai.com
ip.tyk.nu
ident.me
icanhazip.com
bot.whatismyipaddress.com
eth0.me
```

Conclusions

This particular unknown actor is widely using the OSX backdoor described above, blindly spearphishing Windows and Apple systems within targeted organizations. It has been active and unidentified since April 2017. We, and partners, have not observed exploits deployed by the actor.

The group appears to rely on fairly low-tech social engineering delivery, but has actively targeted high-tech organizations for several months. With the active development of the backdoor itself, we expect to observe ongoing activity and targeting from this group.

Appendix I – Indicators of Compromise

Hashes

```
More recent, larger version - 216,370 bytes
f0266724ff69e5ab819e554e33d39042
7578d23e160073cfac6fd65e426c6504

Earlier, smaller version - 190,622 bytes
150e6b91cf714333193f5edfe6c4beef
545aaf30e7f7e1f786257d933b50f2da
895cbb84c7f5eb7fbce79a050c60b823
996cbd807f9aefca71162d11d2484efd
```

Yara

```
private rule Macho_Header
{
meta:
        author = “Kaspersky Lab”
        copyright = “Kaspersky Lab”
         desc = "Macho catch_all"

condition:
        (uint32(0) == 0xFEEDFACF)
        or (uint32(0) == 0xFEEDFACE)
        or (uint32(0) == 0xBEBAFECA)
        or (uint32be(0) == 0xFEEDFACF)
        or (uint32be(0) == 0xFEEDFACE)
        or (uint32be(0) == 0xBEBAFECA)
}

rule apt_ZZ_DEMSTY_persistence
{
meta:
        author = “Kaspersky Lab”
        copyright = “Kaspersky Lab”
        desc = "Exploratory Rule for DEMSTY malware persistence"
        md5 = "545aaf30e7f7e1f786257d933b50f2da"
        version = "1.3"
```

```
strings:
        $persistMust1 = "/System/Library/LaunchDaemons/" ascii wide
        $persistMust2 = "/Library/LaunchDaemons/" ascii wide
        $persistMust3 = "/System/Library/LaunchAgents/" ascii wide
        $persistMust4 = "/Library/LaunchAgents/" ascii wide

        $plistCreate1 = "<?xml version=\"1.0\" encoding=\"UTF-8\"?>" ascii wide
        $plistCreate2 = "<!DOCTYPE plist PUBLIC \"-//Apple//DTD PLIST 1.0//EN\"
\"http://www.apple.com/DTDs/PropertyList-1.0.dtd\">" ascii wide
        $plistCreate3 = "<plist version=\"1.0\">" ascii wide
        $plistCreate4 = "<dict>" ascii wide
        $plistCreate5 = "<key>Disabled</key>" ascii wide
        $plistCreate6 = "<false/>" ascii wide
        $plistCreate7 = "<key>UserName</key>" ascii wide
        $plistCreate8 = "<string>root</string>" ascii wide
        $plistCreate9 = "<key>Label</key>" ascii wide
        $plistCreate10 = "<string>" ascii wide
        $plistCreate11 = "</string>" ascii wide
        $plistCreate12 = "<key>KeepAlive</key>" ascii wide
        $plistCreate13 = "<dict>" ascii wide
        $plistCreate14 = "<key>NetworkState</key>" ascii wide
        $plistCreate15 = "<true/>" ascii wide
        $plistCreate16 = "</dict>" ascii wide
        $plistCreate17 = "<key>ProgramArguments</key>" ascii wide
        $plistCreate18 = "<array>" ascii wide
        $plistCreate19 = "<string>" ascii wide
        $plistCreate20 = "</string>" ascii wide
        $plistCreate21 = "<string>d</string>" ascii wide
        $plistCreate22 = "</array>" ascii wide
        $plistCreate23 = "<key>RunAtLoad</key>" ascii wide
        $plistCreate24 = "<true/>" ascii wide
        $plistCreate25 = "<key>StartInterval</key>" ascii wide
        $plistCreate26 = "<integer>5</integer>" ascii wide
        $plistCreate27 = "</dict>" ascii wide
        $plistCreate28 = "</plist>" ascii wide
        $plistCreate29 = ".plist" ascii wide
        $plistCreate30 = "StartService (){" ascii wide
        $plistCreate31 = "    ConsoleMessage \"Start system Service\"" ascii wide
        $plistCreate32 = "StopService (){" ascii wide
        $plistCreate33 = "return 0" ascii wide
        $plistCreate34 = "RestartService (){" ascii wide
        $plistCreate35 = "return 0" ascii wide
        $plistCreate36 = "RunService \"$1\"" ascii wide
        $plistCreate37 = "    Description     = \"Start systemd\";" ascii wide
        $plistCreate38 = "    Provides        = (\"system\");" ascii wide
        $plistCreate39 = "    Requires        = (\"Network\");" ascii wide
        $plistCreate40 = "    OrderPreference = \"None\";" ascii wide
        $plistCreate41 = "StartupParameters.plist" ascii wide
```

```
condition:
        Macho_Header and
        (all of ($persistMust*))
        and
        (38 of ($plistCreate*))
}

rule apt_ZZ_DEMSTY_placeholders
{
meta:
        author = “Kaspersky Lab”
        copyright = “Kaspersky Lab”
        desc = "Exploratory Rule for DEMSTY malware placeholders"
        md5 = "545aaf30e7f7e1f786257d933b50f2da"
        version = "1.3"

strings:
        $placeholder1 = "%u.%u.%u.%u" ascii wide
        $placeholder2 = "get %s host error" ascii wide
        $placeholder3 = "get %s %s host ok" ascii wide
        $placeholder4 = "%04x%04x" ascii wide
        $placeholder5 = "%u_%04u_%04u" ascii wide
        $placeholder7 = "exec failed %s" ascii wide
        $placeholder8 = "<key>%s</key>" ascii wide

condition:
        Macho_Header and
        7 of ($placeholder*)
}

rule apt_ZZ_DEMSTY_errors
{
meta:
        author = “Kaspersky Lab”
        copyright = “Kaspersky Lab”
        desc = "Exploratory Rule for DEMSTY malware errors"
        md5 = "545aaf30e7f7e1f786257d933b50f2da"
        version = "1.3"

strings:
        $errorMsg1 = "This file is corrupted and connot be opened" ascii wide
        $errorMsg2 = "start plugin process failed" ascii wide
        $errorMsg3 = "wait plugin process failed" ascii wide
        $errorMsg4 = "copy plugin to bin path failed" ascii wide
        $errorMsg5 = "not found plugin state" ascii wide
        $errorMsg7 = "exe new version failed" ascii wide
```

```
condition:
      Macho_Header and any of ($errorMsg*)
}

rule apt_ZZ_DEMSTY_myIP
{
meta:
       author = “Kaspersky Lab”
       copyright = “Kaspersky Lab”
       desc = "Exploratory Rule for DEMSTY malware IP check"
       md5 = "545aaf30e7f7e1f786257d933b50f2da"
       version = "1.3"

strings:
       $hostpostproc = "hostname |cut -d '.' -f1" ascii wide

       $whatismyip2 = "whatismyip.akamai.com" ascii wide
       $whatismyip3 = "ip.tyk.nu" ascii wide
       $whatismyip4 = "ident.me" ascii wide
       $whatismyip5 = "icanhazip.com" ascii wide
       $whatismyip6 = "bot.whatismyipaddress.com" ascii wide
       $whatismyip7 = "eth0.me" ascii wide

condition:
        Macho_Header and
       $hostpostproc and (4 of ($whatismyip*))
}

rule apt_ZZ_DEMSTY_commands
{
meta:
       author = “Kaspersky Lab”
       copyright = “Kaspersky Lab”
       desc = "Exploratory Rule for DEMSTY malware commands"
       md5 = "545aaf30e7f7e1f786257d933b50f2da"
       version = "1.3"

strings:
       $cmd1 = "sysctl -a |grep machdep.cpu.brand_string|cut -d ':' -f2" ascii wide
       $cmd2 = "sysctl -a |grep hw.memsize: |cut -d ':' -f2" ascii wide
       $cmd3 = "chflags uchg " ascii wide
       $cmd4 = ";chflags  schg " ascii wide
       $cmd5 = ";chflags hidden " ascii wide
       $cmd6 = "chflags nouchg " ascii wide
       $cmd7 = ";chflags  noschg " ascii wide
       $cmd8 = ";chflags nohidden " ascii wide
```

```
        $cmd9 = "hostname |cut -d '.' -f1" ascii wide

condition:
        all of them
}

rule apt_ZZ_DEMSTY_encryptedStrings
{
meta:
        author = “Kaspersky Lab”
        copyright = “Kaspersky Lab”
        desc = "Exploratory Rule for DEMSTY malware encrypted strings, XOR 0x59"
        md5 = "545aaf30e7f7e1f786257d933b50f2da"
        version = "1.3"

strings:
        $encrypted1 = "v-4)vw* *-<4=v" ascii wide
        $encrypted2 = "* *-<4=w56:2" ascii wide
        $encrypted3 = "* *-<4" ascii wide
        $encrypted4 = ",)>+8=<" ascii wide
        $encrypted5 = ")5,>07!!!w-4)" ascii wide
        $encrypted6 = "vw56:85v;07v2< ;68+=04<" ascii wide
        $encrypted7 = "vw56:85v;07v* *<-4=" ascii wide
        $encrypted8 = "0;+8+ v* *<-4=" ascii wide
        $encrypted9 = "0;+8+ v2< ;68+=04<" ascii wide
        $encrypted10 = "v-4)vw2;=+t,70!v2;=04<w56:2" ascii wide
        $encrypted11 = "vw56:85vw* *-<4=v* *-<4=w,70(" ascii wide

condition:
       Macho_Header and 8 of ($encrypted*)
}

rule apt_ZZ_DEMSTY_failures
{
meta:
        author = “Kaspersky Lab”
        copyright = “Kaspersky Lab”
        desc = "Exploratory Rule for DEMSTY malware fail strings"
        md5 = "545aaf30e7f7e1f786257d933b50f2da"
        version = "1.3"

strings:
        $failure1 = ":open failed:" ascii wide
        $failure2 = ":not exist" ascii wide
        $failure3 = ":open file failed" ascii wide
        $failure4 = ":pos or size error" ascii wide
        $failure5 = ":get filesize failed" ascii wide
        $failure6 = ":getoffset or block failed" ascii wide
        $failure7 = ":delete failed" ascii wide
        $failure8 = "set failed" ascii wide
        $failure9 = "get content failed" ascii wide

condition:
       Macho_Header and 7 of ($failure*)
}

rule apt_ZZ_DEMSTY_standout
{
meta:
        author = “Kaspersky Lab”
        copyright = “Kaspersky Lab”
        desc = "Exploratory Rule for DEMSTY malware standout strings"
        md5 = "545aaf30e7f7e1f786257d933b50f2da"
        version = "1.3"

strings:
        $standout1 = "sysctl -a |grep machdep.cpu.brand_string|cut -d ':' -f2" ascii
wide
        $standout2 = "sysctl -a |grep hw.memsize: |cut -d ':' -f2" ascii wide
        $standout3 = "%upgrade%" ascii wide
        $standout4 = "%keymod%" ascii wide
        $standout5 = "hostname |cut -d '.' -f1" ascii wide
        $standout6 = "This file is corrupted and connot be opened" ascii wide
        $standout7 = "not found plugin state" ascii wide
        $standout8 = "exe new version failed" ascii wide
        $standout9 = "ip.tyk.nu" ascii wide

condition:
        Macho_Header and any of them
}
```