Lethic Botnet Returns, Uses "Realtek" Identifier

zscaler.com/blogs/security-research/lethic-botnet-returns-uses-realtek-identifier

Zscaler Blog

Get the latest Zscaler blog updates in your inbox

Subscribe

Security Research

image

Remember Stuxnet? Chances are you do- a few months back there was a worm that spread over USB using the 0-day .LNK vulnerability (CVE-2010-2568) and targeted Siemens SCADA systems. Additionally the rootkit package that it installed was digitally signed using real certificates from real hardware manufacturers: Realtek Semiconductor Corp. (realtek.com.tw) was one of the companies (JMicron was the other - both are Taiwanese companies).

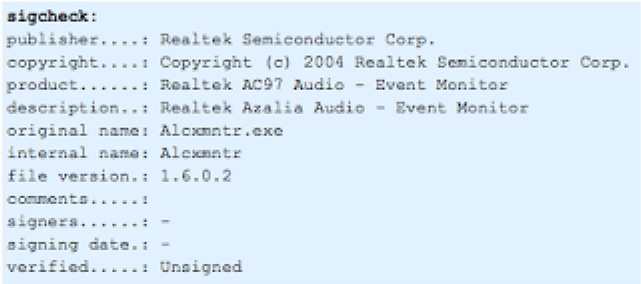
In recent days, I have seen malware with Realtek Semiconductor Corp. signature information. Specifically, it has been of the Trojan Lethic / Ddox malware family. About a year ago, Jose Nazario detailed his analysis on the Lethic bot being used to spew pharma, replica, etc. spam. About a month after he posted his analysis, M86 reported on the Lethic botnet takedown. Well it appears that there is a new variant / botnet of this malware family:

Here are two recent samples:

MD5: 0460d89f0091d951184a8d77c6641340
First seen: 2010-10-31 17:42:29
VirusTotal Report

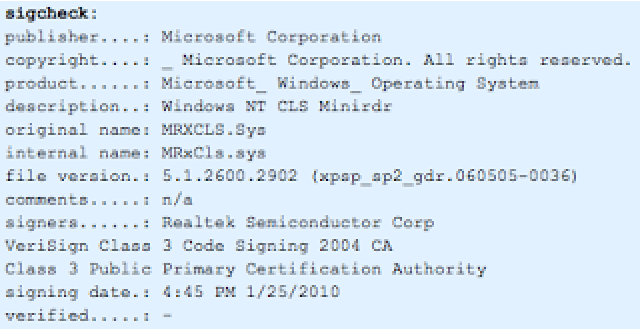
MD5: ddb7aee9b335f479e0e2ac7aaf223856
First seen: 2010-11-07 09:58:39
VirusTotal Report

Both have Realtek information reported from Microsoft's Sigcheck tool:



```
sigcheck:
publisher....: Realtek Semiconductor Corp.
copyright....: Copyright (c) 2004 Realtek Semiconductor Corp.
product......: Realtek AC97 Audio - Event Monitor
description..: Realtek Azalia Audio - Event Monitor
original name: Alcxmntr.exe
internal name: Alcxmntr
file version.: 1.6.0.2
comments.....:
signers......: -
signing date.: -
verified.....: Unsigned
```

However, the tool shows no signer / certificate authority verified the signature. Here is a snapshot of the Stuxnet signcheck output for comparison:

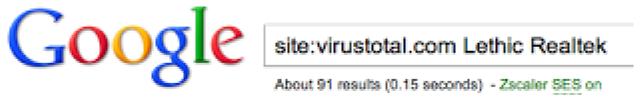


```
sigcheck:
publisher....: Microsoft Corporation
copyright....: _ Microsoft Corporation. All rights reserved.
product......: Microsoft_ Windows_ Operating System
description..: Windows NT CLS Minirdr
original name: MRXCLS.Sys
internal name: MRxCls.sys
file version.: 5.1.2600.2902 (xpsp_sp2_gdr.060505-0036)
comments.....: n/a
signers......: Realtek Semiconductor Corp
VeriSign Class 3 Code Signing 2004 CA
Class 3 Public Primary Certification Authority
signing date.: 4:45 PM 1/25/2010
verified.....: -
```

Stuxnet and Lethic are completely different, and I am in no way presuming that one or more authors behind either malware campaign intersect - I did think it was interesting that this one company is being "picked" in malware campaigns though.

There may be some correlation with the exact Realtek information in the Lethic binary. The information within the Lethic binary does appear to mimic valid Realtek information for their AC97 Audio product. Doing some searches, I've found other malware families have used this exact Realtek information within their malware binaries. Here is a VirusTotal report from an SDBot sample first seen in January 2010, that has the exact same Realtek information used by Lethic. Separate malware authors could have simply selected a legitimate software package and included the exact information - however this does seem pretty coincidental. Or perhaps it could be the "signature" of a common author or group behind these artifacts - perhaps they seek to tarnish the reputation of this Taiwanese company for personal or political motivation - who knows?

There are about 91 Lethic samples with the "Realtek" signature information that Google shows from VirusTotal. These date from early September to present.



site:virustotal.com Lethic Realtek

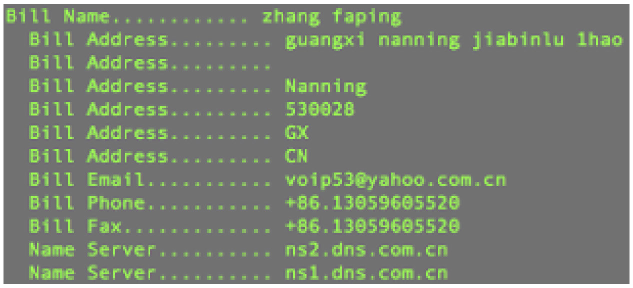
About 91 results (0.15 seconds) - Zscaler SES on

In the past few days, locations that I've seen the Lethic bot spread from include:
77.79.9.174 over port 17678
85.17.58.165 over port 36182
91.121.175.219 over port 16512

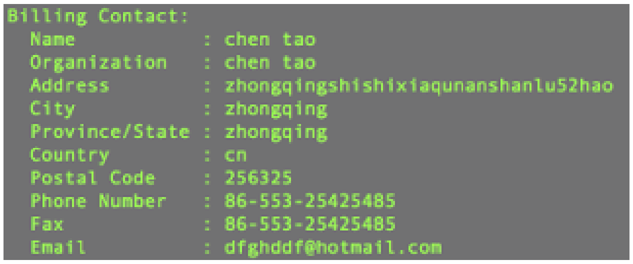
The port location changes over time, and rotates through funky sounding executable names that appear to be auto-generated from various letter permutations. For example:
bknx.exe
fewfdewwe.exe
fefewwew.exe
rfvmimikwe.exe
vgewfwqwq.exe
vgrwvew.exe

Following infection, connection attempts have been seen to:
izuhjsn.com (173.236.56.218) on port 8706
xkihjhx.com (67.159.45.104) on port 2904

The domains were both registered August 1, 2010 through the Registrars:
BEIJING INNOVATIVE LINKAGE TECHNOLOGY LTD. DBA DNS.COM.CN,
XIN NET TECHNOLOGY CORPORATION



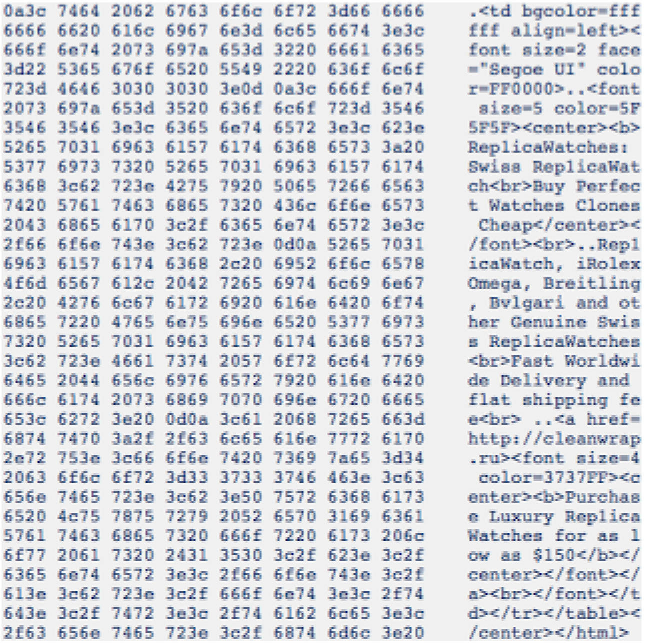
```
Bill Name............ zhang faping
  Bill Address......... guangxi nanning jiabinlu 1hao
  Bill Address.........
  Bill Address......... Nanning
  Bill Address......... 530028
  Bill Address......... GX
  Bill Address......... CN
  Bill Email........... voip53@yahoo.com.cn
  Bill Phone........... +86.13059605520
  Bill Fax............. +86.13059605520
  Name Server.......... ns2.dns.com.cn
  Name Server.......... ns1.dns.com.cn
```



```
Billing Contact:
  Name           : chen tao
  Organization   : chen tao
  Address        : zhongqingshishixiaqunanshanlu52hao
  City           : zhongqing
  Province/State : zhongqing
  Country        : cn
  Postal Code    : 256325
  Phone Number   : 86-553-25425485
  Fax            : 86-553-25425485
  Email          : dfghddf@hotmail.com
```

DomainTools shows 12 other registered domains with the "voip53" Yahoo email address and 62 other registered domains with the "dfghddf" Hotmail email address within the whois information - presumably other malicious / C&C domains.

In mid-October, an Anubis report shows a "Realtek" Lethic sample looping through a number of SMTP proxies/open-relays and sending spam similar to the pharma, replicas, etc. that Jose had reported in the previous 2009 iteration of the botnet. Here is a pcap snapshot of a replica spam message sent from the recent, Fall 2010 iteration of the Lethic bot:



```
0a3c 7464 2062 6763 6f6c 6f72 3d66 6666    .<td bgcolor=fff
6666 6620 616c 6967 6e3d 6c65 6674 3e3c    fff align=left><
666f 6e74 2073 697a 653d 3220 6661 6365    font size=2 face
3d22 5365 676f 6520 5549 2220 636f 6c6f    ="Segoe UI" colo
723d 4646 3030 3030 3e0d 0a3c 666f 6e74    r=FF0000>..<font
2073 697a 653d 3520 636f 6c6f 723d 3546     size=5 color=5F
3546 3546 3e3c 6365 6e74 6572 3e3c 623e    5F5F><center><b>
5265 7031 6963 6157 6174 6368 6573 3a20    ReplicaWatches: 
5377 6973 7320 5265 7031 6963 6157 6174    Swiss ReplicaWat
6368 3c62 723e 4275 7920 5065 7266 6563    ch<br>Buy Perfec
7420 5761 7463 6865 7320 436c 6f6e 6573    t Watches Clones
2043 6865 6170 3c2f 6365 6e74 6572 3e3c     Cheap</center><
2f66 6f6e 743e 3c62 723e 0d0a 5265 7031    /font><br>..Repl
6963 6157 6174 6368 2c20 6952 6f6c 6578    icaWatch, iRolex
4f6d 6567 612c 2042 7265 6974 6c69 6e67    Omega, Breitling
2c20 4276 6c67 6172 6920 616e 6420 6f74    , Bvlgari and ot
6865 7220 4765 6e75 696e 6520 5377 6973    her Genuine Swis
7320 5265 7031 6963 6157 6174 6368 6573    s ReplicaWatches
3c62 723e 4661 7374 2057 6f72 6c64 7769    <br>Fast Worldwi
6465 2044 656c 6976 6572 7920 616e 6420    de Delivery and 
666c 6174 2073 6869 7070 696e 6720 6665    flat shipping fe
653c 6272 3e20 0d0a 3c61 2068 7265 663d    e<br> ..<a href=
6874 7470 3a2f 2f63 6c65 616e 7772 6170    http://cleanwrap
2e72 753e 3c66 6f6e 7420 7369 7a65 3d34    .ru><font size=4
2063 6f6c 6f72 3d33 3733 3746 463e 3c63     color=3737FF><c
656e 7465 723e 3c62 3e50 7572 6368 6173    enter><b>Purchas
6520 4c75 7875 7279 2052 6570 3169 6361    e Luxury Replica
5761 7463 6865 7320 666f 7220 6173 206c    Watches for as l
6f77 2061 7320 2431 3530 3c2f 623e 3c2f    ow as $150</b></
6365 6e74 6572 3e3c 2f66 6f6e 743e 3c2f    center></font></
613e 3c62 723e 3c2f 666f 6e74 3e3c 2f74    a><br></font></t
643e 3c2f 7472 3e3c 2f74 6162 6c65 3e3c    d></tr></table><
2f63 656e 7465 723e 3c2f 6874 6d6c 3e20    /center></html>
```

El Reg recently reported on how prolific the Lethic botnet was and the success of the takedown... could it be ramping up to make a come back? Also, can this "Realtek" signature info be used to tie the author/group to the malware they have released?

Update:
The Sigcheck tool apparently parses the PE File Version Info data structure and includes this in the output. The above "Realtek" information is actually extracted from the PE File Version Info data structure (e.g., here). While this is not a digital signature- it is still identifying info that may be able to tie certain malware samples to the same author / group / or binary builder.

Thank you for reading

Was this post useful?

Yes, very!Not really

Get the latest Zscaler blog updates in your inbox