Additional information regarding the recent CCleaner APT security incident

blog.avast.com/additional-information-regarding-the-recent-ccleaner-apt-security-incident

New analysis from the Avast Threat Labs

We would like to update our customers and the general public on the latest findings regarding the investigation of the recent CCleaner security incident. As published in our previous blog posts (here and here), analysis of the CnC server showed that the incident was in fact an Advanced Persistent Threat (APT) attack, targeting specific high-tech and telecommunications companies. That is, despite the fact that CCleaner is a consumer product, the purpose of the attack was not to attack consumers and their data; instead, the CCleaner customers were used to gain access to corporate networks of select large enterprises.

Today, we are going to disclose new facts about the incident that we received since the last public update.

Introduction

As we already know, the CnC server contained important evidence in terms of the exact list of hosts with which the CnC server communicated, and the list of hosts to which it actually sent the 2nd stage payload (i.e. which actually became compromised in the sense that they could execute malicious code sent by the attacker). The problem was that due to a crash of

the database, there were only about 3.5 days' worth of data. Our hypothesis was that this occurred because of the server running out of disk space on September 10, leading the operator to a full rebuild of the database.

However, further investigation revealed that the attackers backed up the data from the crashed CnC server to another server before rebuilding the database. Thanks to the continued work of the Avast Threat Labs team and the help from US law enforcement personnel. The server's IP address was 216.126.225.163, it featured the same self-signed SSL certificate (issued for speccy.piriform.com) and stack-wise, had a typical "LAMP" configuration: CentOS release 6.9 with Apache 2.2.15, PHP 5.3.3, but most importantly, a MySql database that turned out to contain data going back to August 18. Access to this backup server allowed us to assemble what we believe is the complete database (the only missing piece is a 40-hour window between 2017-09-10 19:03:18 and 2017-09-12 9:58:47 UTC, i.e. between the crash of the original CnC DB and the creation of the new one; it is not clear how the CnC server behaved in that period).

The main findings from the complete database are as follows:

- The total number of connections to the CnC server was 5,686,677.
- The total number of unique PCs (unique MAC addresses) that communicated with the CnC server was 1,646,536.
- The total number of unique PCs that received the 2nd stage payload was 40.

PCs and Companies that received the 2nd stage payload

The most important piece of information is the content of the "OK" table in the database, which lists the machines that successfully received the 2nd stage payload and were therefore really "infected" with potentially malicious code (although we haven't been able to isolate that code yet, as it probably came from additional layers which are still the focus of additional investigation).

Here is the complete list of companies / domains affected, together with the number of impacted PCs:

Domain	Industry	Country	Number of impacted PCs
cht.com.tw	Telco	Taiwan	13
nsl.ad.nec.co.jp	Tech	Japan	10
samsung samsung.sk samsung.sepm	Tech	Korea	5
corpnet.asus paskey.corpnet.asus	Tech	Taiwan	2
ad.fip.fujitsu.com domain.ftsp.ten.fujitsu.com	Tech	Japan	2
am.sony.com	Tech	Japan	2
infoview2u.dvrdns.org	Internet	USA	1
uk.pri.o2.com	Telco	UK	1
gg.gauselmann.com	Gaming	Germany	1
singtel	Telco	Singapore	1
intel.com	Tech	USA	1
vmware.com	Tech	USA	1

We have reached out to all these companies, with the aim of providing them with detailed information about the incident, list of impacted computers, and additional IOCs that can be used to detect the infection and take corrective actions.

Worth noting is that about 40 PCs out of 2.27M had the compromised version of CCleaner product installed, i.e. 0.0018% of the total -- a truly targeted attack.

The list of companies (domains) evolved over time, and the detailed logs found on the SQL database server suggest that the bad actors were trying to identify suitable hosts not just by a pre-determined list, but also by looking into what kind of PC hosts have actually been available to them in the sense that they had PCs with CCleaner connecting to the CnC. Following is a list of targets that were of potential interest, but were not attacked by the 2nd stage payload:

Domain	Industry	Country	Number of impacted PCs
htcgroup.corp	Tech	Taiwan	0
linksys	Tech	USA	0
apo.epson.net	Tech	Japan	0
vf-es.internal.vodafone.com	Telco	UK	0
ntdev.corp.microsoft.com	Tech	USA	0
dlink.com	Tech	Taiwan	0
hq.gmail.com	Tech	USA	0
dfw01.corp.akamai.com	Internet	USA	0
msi.com.tw	Tech	Taiwan	0
cisco.com	Tech	USA	0
cyberdyne.jp cyberdyne.local cyberdyne.root	Tech	Japan	0
tti-ecm.local tti.local tti.on.ca	Military	Canada	0
godaddy	Internet	USA	0

Clearly, the logs also indicate that the attackers were looking for additional high-profile companies to target, some of them potentially leading to additional supply-chain attacks (Carriers / ISPs, server hosting companies and domain registrars).

Interestingly enough, the two corporations with the highest number of impacted PCs (cht.com.tw and nsl.ad.nec.co.jp) were actually missing in the list of targeted domains on the CnC server at the time it was taken down. This suggests that the attackers actively removed these companies from the list after the payload had been delivered.

Origin of the attacker

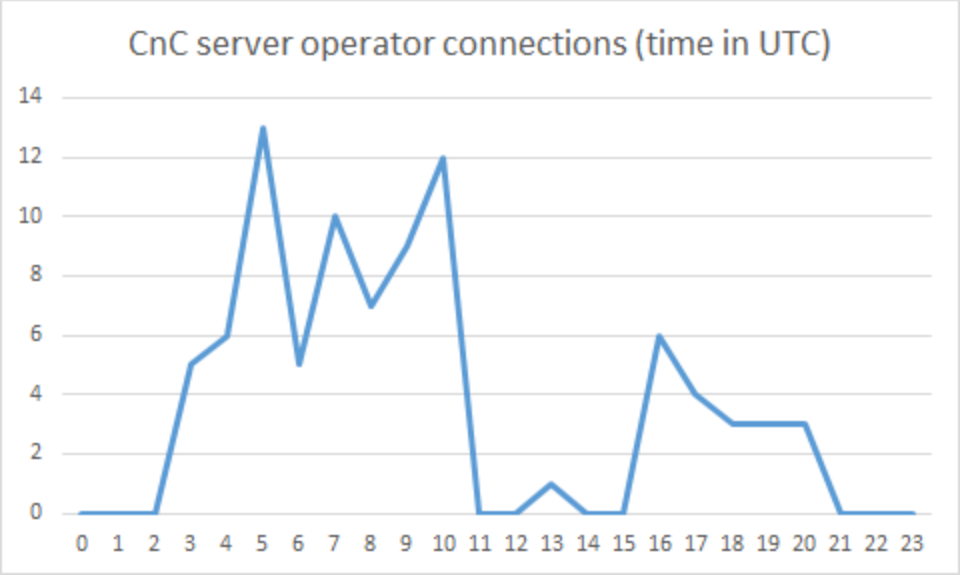
In the previous post, we talked about the fact that there were multiple clues suggesting that the attack may be originating from China, including multiple instances of PHP code found on the CnC server, the myPhpAdmin logs, and the similarity of certain code snippets to a previous APT attack attributed to China.

The problem with all these indications is that they are all very easy to forge: they might have been added simply to make investigation more difficult and to hide the true origin.

So, during our investigation, we tried to take a slightly different approach. We noticed that there have been a relatively large number of operator connections to the CnC server; the server apparently required a lot of manual maintenance work. In total, the operator connected to the server 83 times (plus 17 more times to the backup server), to do various things from installing and setting up the systems to monitoring it and resolving respective issues, such as to fix the crashed database. Which made us think that this was in fact someone's 'day job'. The hypothesis was further supported by the fact that there were many fewer connections to the server on Saturdays, and almost no connections on Sundays.

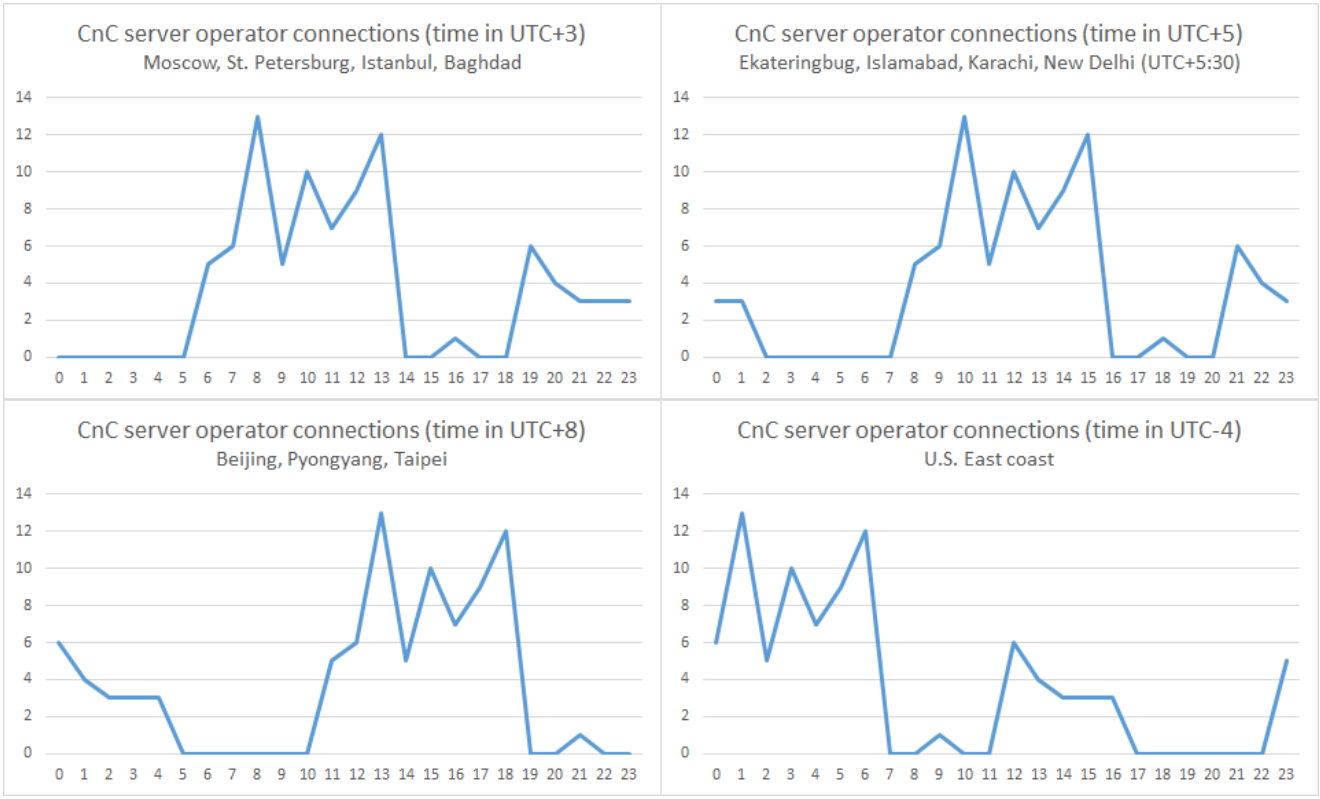
Now, with that hypothesis in place, the obvious thing to do was to plot the operator connections to the server in a chart and try to determine the time zone in which the attacker resided.

The result looked like this:



There is a clear pattern, which is in fact quite typical for IT workers: an 8-hour working day, followed by 4-5 hours of inactivity in the afternoon/evening and then additional connections during a 5-hour block in the evenings.

Given the typical working day starts at 8AM or 9AM, this leads us to the most likely location of the attacker in the time zone UTC + 4 or UTC + 5, leading us to Russia or the eastern part of Middle East / Central Asia and India. Furthermore, given the clear lack of traffic on Saturdays and Sundays, it would indicate that it wasn't an Arabic country.



Another possible explanation is that there were multiple people involved in the operation, each working from a different time zone.

It is worth noting that, despite there being a large number of tech / telco companies in China, Russia and India, there are no companies from these countries on the list of companies targeted by this attack.

Investigation process and next steps

We are continuing our investigation of the incident: working with law enforcement, partner companies and a professional firm specializing in incident response operations to move quickly in the right direction. Our security team has reached out to all companies proven to be part of the 2nd stage, and we're committed to working with them to resolve the issue fully. Obviously, the fact that the 2nd stage payload has been delivered to a computer connected to a company network doesn't mean that the company network has been compromised. However, proper investigation is in order and necessary to fully understand the impact and take remediation actions. From our side, we continue working on getting access and analyzing the additional stages of the payload (post stage 2). We will post an update as soon as we learn more.

IOCs

The following is an updated list of IOCs.

Files

1st stage

04bed8e35483d50a25ad8cf203e6f157e0f2fe39a762f5fbacd672a3495d6a11 - CCleaner - installer (v5.33.0.6162)

0564718b3778d91efd7a9972e11852e29f88103a10cb8862c285b924bc412013 - CCleaner - installer (v5.33.0.6162)

1a4a5123d7b2c534cb3e3168f7032cf9ebf38b9a2a97226d0fdb7933cf6030ff - CCleaner - installer (v5.33.0.6162)

276936c38bd8ae2f26aab14abff115ea04f33f262a04609d77b0874965ef7012 - CCleaner - installer (v5.33.0.6162)

2fe8cfeeb601f779209925f83c6248fb4f3bfb3113ac43a3b2633ec9494dcee0 - CCleaner - installer (v5.33.0.6162)

3c0bc541ec149e29afb24720abc4916906f6a0fa89a83f5cb23aed8f7f1146c3 - CCleaner - installer (v5.33.0.6162)

4f8f49e4fc71142036f5788219595308266f06a6a737ac942048b15d8880364a - CCleaner - installer (v5.33.0.6162)

7bc0eaf33627b1a9e4ff9f6dd1fa9ca655a98363b69441efd3d4ed503317804d - CCleaner - installer (v5.33.0.6162)

a013538e96cd5d71dd5642d7fdce053bb63d3134962e2305f47ce4932a0e54af - CCleaner - installer (v5.33.0.6162)

bd1c9d48c3d8a199a33d0b11795ff7346edf9d0305a666caa5323d7f43bdcfe9 - CCleaner - installer (v5.33.0.6162)

c92acb88d618c55e865ab29caafb991e0a131a676773ef2da71dc03cc6b8953e - CCleaner - installer (v5.33.0.6162)

e338c420d9edc219b45a81fe0ccf077ef8d62a4ba8330a327c183e4069954ce1 - CCleaner - installer (v5.33.0.6162)

36b36ee9515e0a60629d2c722b006b33e543dce1c8c2611053e0651a0bfdb2e9 - CCleaner.exe (32-bit v5.33.0.6162)

6f7840c77f99049d788155c1351e1560b62b8ad18ad0e9adda8218b9f432f0a9 - CCleaner.exe (32-bit v5.33.0.6162)

a3e619cd619ab8e557c7d1c18fc7ea56ec3dfd13889e3a9919345b78336efdb2 - CCleanerCloud - installer (32-bit v1.7.0.3191)

0d4f12f4790d2dfef2d6f3b3be74062aad3214cb619071306e98a813a334d7b8 - CCleanerCloudAgent.exe (32-bit v1.7.0.3191)

9c205ec7da1ff84d5aa0a96a0a77b092239c2bb94bcb05db41680a9a718a01eb - CCleanerCloudAgentHealtCheck.exe (32-bit v1.7.0.3191)

bea487b2b0370189677850a9d3f41ba308d0dbd2504ced1e8957308c43ae4913 - CCleanerCloudTray.exe (32-bit v1.7.0.3191)

3a34207ba2368e41c051a9c075465b1966118058f9b8cdedd80c19ef1b5709fe - 1st stage payload DLL found in CCleaner

19865df98aba6838dcc192fbb85e5e0d705ade04a371f2ac4853460456a02ee3 - 1st stage payload DLL found in CCleanerCloud

2nd stage

dc9b5e8aa6ec86db8af0a7aa897ca61db3e5f3d2e0942e319074db1aaccfdc83 - 2nd stage payload DLL (GeeSetup_x86.dll)
a414815b5898ee1aa67e5b2487a11c11378948fcd3c099198e0f9c6203120b15 - loader of the 2nd stage payload (64-bit)
7ac3c87e27b16f85618da876926b3b23151975af569c2c5e4b0ee13619ab2538 - loader of the 2nd stage payload (32-bit)
4ae8f4b41dcc5e8e931c432aa603eae3b39e9df36bf71c767edb630406566b17 - inner DLL of the 2nd stage payload (64-bit)
b3badc7f2b89fe08fdee9b1ea78b3906c89338ed5f4033f21f7406e60b98709e - inner DLL of the 2nd stage payload (32-bit)
a6c36335e764b5aae0e56a79f5d438ca5c42421cae49672b79dbd111f884ecb5 - inner DLL of the 2nd stage payload (32-bit)

CnC

IPs

216.126.225.148 - CnC of the 1st stage payload

216.126.225.163 - backup server of CnC 216.126.225.148

URLs (all used for obtaining IP address of the 2nd stage CnC)

get.adoble[.]com

https://github[.]com/search?q=joinlur&type=Users&u= ✓

https://en.search.wordpress[.]com/?src=organic&q=keepost

DGA (used by the 1st stage payload)

ab8cee60c2d.com - valid for 2017-08

ab1145b758c30.com - valid for 2017-09

ab890e964c34.com - valid for 2017-10

ab3d685a0c37.com - valid for 2017-11

ab70a139cc3a.com - valid for 2017-12

ab3c2b0d28ba6.com - valid for 2018-01

ab99c24c0ba9.com - valid for 2018-02

ab2e1b782bad.com - valid for 2018-03

ab253af862bb0.com - valid for 2018-04

ab2d02b02bb3.com - valid for 2018-05

ab1b0eaa24bb6.com - valid for 2018-06

abf09fc5abba.com - valid for 2018-07

abce85a51bbd.com - valid for 2018-08

abccc097dbc0.com - valid for 2018-09

ab33b8aa69bc4.com - valid for 2018-10

ab693f4c0bc7.com - valid for 2018-11

ab23660730bca.com - valid for 2018-12

Windows Registry

HKLM\SOFTWARE\Piriform\Agomo\MUID - used by the 1st stage payload

HKLM\SOFTWARE\Piriform\Agomo\NID - used by the 1st stage payload

HKLM\SOFTWARE\Piriform\Agomo\TCID - used by the 1st stage payload

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\WbemPerf\HBP - used by the 2nd stage payload

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\WbemPerf\001 - used by the 2nd stage payload

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\WbemPerf\002 - used by the 2nd stage payload

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\WbemPerf\003 - used by the 2nd stage payload

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\WbemPerf\004 - used by the 2nd stage payload