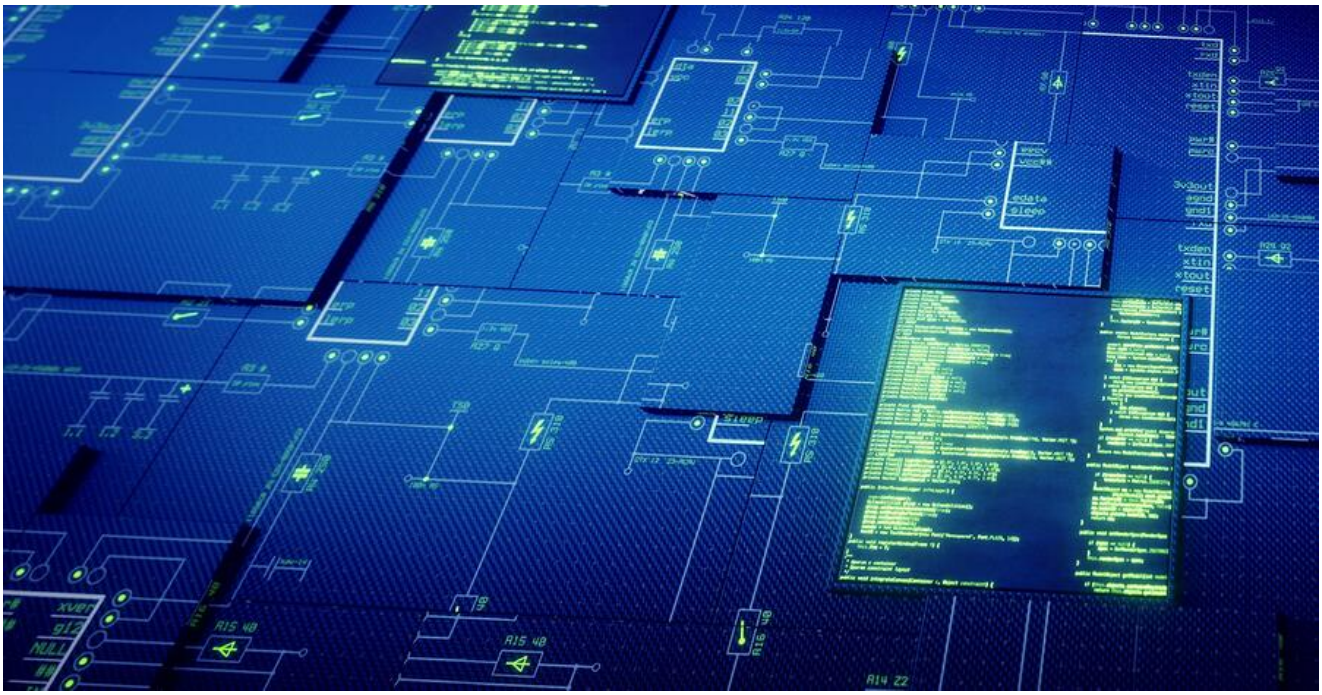
Recent findings from CCleaner APT investigation reveal that attackers entered the Piriform network via TeamViewer

blog.avast.com/update-ccleaner-attackers-entered-via-teamviewer



Ondrej Vlcek 18 Apr 2018

Unrelated to the CCleaner attack, Avast also found ShadowPad samples active in South Korea and Russia, logging a financial transaction

Today, I shared new findings from Avast's continued investigations of the CCleaner APT (Advanced Persistent Threat) at RSA.

Last September, we disclosed that CCleaner had been targeted by cybercriminals, in order to distribute malware via the CCleaner installation file. The modified installation file was downloaded by 2.27 million CCleaner customers worldwide. Thereafter, our threat intelligence team has been investigating what happened.

Since the update we gave at SAS last month, we have made further discoveries about how the attackers infiltrated the Piriform network and the tactics they used to fly under the radar. As we looked for similarities with other attacks, we also analyzed older versions of

ShadowPad, the cyber attack platform we had found on four Piriform computers. Our investigation revealed that ShadowPad had been previously used in South Korea, and in Russia, where attackers intruded a computer, observing a money transfer.

CCleaner attack: How the threat actors got into the Piriform network

To initiate the CCleaner attack, the threat actors first accessed Piriform's network on March 11, 2017, four months before Avast acquired the company, using TeamViewer on a developer workstation to infiltrate. They successfully gained access with a single sign-in, which means they knew the login credentials. While we don't know how the attackers got their hands on the credentials, we can only speculate that the threat actors used credentials the Piriform workstation user utilized for another service, which may have been leaked, to access the TeamViewer account.

According to the log files, TeamViewer was accessed at 5 AM local time, when the PC was unattended, but running. The attackers tried to install two malicious dlls, however, the attempts were unsuccessful due to lack of admin rights to the system. On the third try, the attackers succeeded to drop the payload, using VBScript, the scripting language developed by Microsoft.

```
2017-03-11 05:02:39         Event Log:TeamViewer UDP: punch received a=*.*.*.*:64002: (*)
2017-03-11 05:03:48         Event Log:TeamViewer FileWriter: Could not create file C:\Users\x64.dll, Errorcode=5
2017-03-11 05:04:03         Event Log:TeamViewer FileWriter: Could not create file C:\Users\x64.dll, Errorcode=5
2017-03-11 05:04:50         Event Log:TeamViewer FileWriter: Could not create file C:\Users\x64.vbs, Errorcode=5
2017-03-11 05:07:31         Jump List:MRUTime    C:\Users\*********\x64.vbs
2017-03-11 05:07:38         Registry             {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}\wscript.exe


2017-03-12 04:12:36         Event Log:TeamViewer "AddParticipant: [705042190,-1697811015] type=6 name=WIN-FC74JD6H4RJ"
                                                 "AddParticipant: [252978432,-1122679512] type=3 name=*********"

2017-03-12 04:12:40         Event Log:TeamViewer "UDP: punch received a=*.*.*.*::63752: (*)"
2017-03-12 04:13:44         Event Log:TeamViewer "ParticipantRemoved: Our own participant was removed,
                                                 we must terminate our session"
```

How attackers tried to get into the 1st computer

The next day, March 12, 2017, the attackers moved laterally onto a second computer, again targeting an unattended computer outside of work hours (4 AM local time). The attackers opened a backdoor through Microsoft's Remote Desktop Service, delivering a binary and payload to the computer's registry. The payload delivered was an older version of the second stage malware, which was delivered to 40 CCleaner users.

```
2017-03-12 04:19:08           File System:Create            C:\windows\prefetch\consent.exe-2D674CE4.pf
2017-03-12 04:19:09           Registry:Modified:UserAssist            C:\ProgramData\CBCB.exe

2017-03-12 04:33:18 Registry:Modified   SOFTWARE\ODBC\ODBC.INI

2017-03-12 04:34:38 Event Log:TS-RCM:1143         The "Limit the size of the entire roaming profile cache"
                    Group Policy setting has been disabled
2017-03-12 04:34:43 Registry:Modified   SYSTEM\ControlSet001\services\SessionEnv
2017-03-12 04:34:43 Event Log:System:7040         Remote Desktop Configuration Service changed from demand start to auto
start

2017-03-12 08:05:48 Registry:Modified   SOFTWARE\Microsoft\Windows NT\CurrentVersion\WbemPerf modified
```

Lateral movement to second computer on March 12

Two days later, the attackers went back to the first computer, also infecting it with the older version of the second stage malware.

```
2017-03-14 01:25:50 File System:Create  C:\windows\system32\TSMSISrv.dll
2017-03-14 01:26:00 Registry:Modified   SOFTWARE\ODBC\ODBC.INI
2017-03-14 01:30:00 Registry:Modified   SYSTEM\ControlSet001\services\SessionEnv
2017-03-14 01:30:44 Registry:Modified   SYSTEM\ControlSet001\services\Schedule
```

The attackers moved back to the first computer, infecting it with older version of the second stage malware

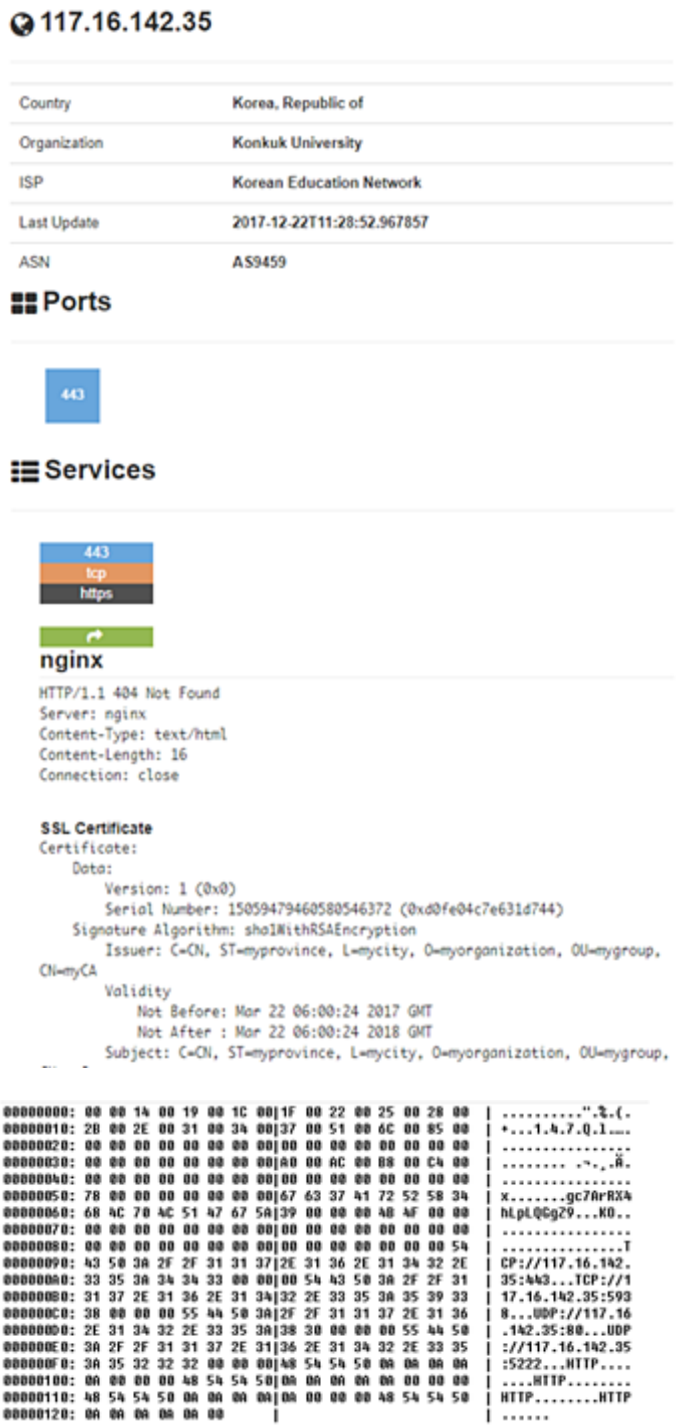
After several weeks of apparent inactivity, the next stage of the payload was delivered to the first infected computer. We believe that the threat actors prepared the malicious binaries during the period of inactivity. The attackers applied several techniques to infiltrate other computers in the internal network, including using passwords gathered by the keylogger, and logging in with administrative privileges through the Windows Remote Desktop application. The payload delivered was the infamous ShadowPad, which we believe was intended as the third stage of the CCleaner attack. It was delivered as a mscoree.dll library to four computers in the Piriform network, including a build server, masking as a .NET runtime library to go unnoticed. This library, which was stored on the disk, had a time stamp on it, revealing that the version of ShadowPad we found was compiled on April 4, 2017. This was just eight days before it was installed on the Piriform computers, meaning it was customized for the attack, which we also described in earlier blog posts in March and September.

The attackers were in the Piriform network five months before they snuck the malicious payload into the CCleaner build. Avast acquired Piriform on July 18, 2017 and the first CCleaner build with the malicious payload appeared on August 2, 2017. It's interesting it took them so long before they initiated their attack on CCleaner users.

ShadowPad active in South Korea and Russia

After analyzing the ShadowPad executable from the Piriform network, we looked for similar files on VirusTotal. We found two samples, one that appeared in South Korea and the other in Russia.

The sample that was uploaded to VirusTotal from South Korea was uploaded on December 27, 2017. It was created to communicate with CnC servers hosted by Konkuk University in South Korea, probably on a hacked PC. Based on how the sample was uploaded and the information included, we think a user uploaded it to VirusTotal, rather than a security company.



left: *decrypted configuration of the virus showing the IP address used in the attack; image credit: Avast*
right: *Images from Internet search engine Shodan.io, showing the services available on the CnC server's IP address; image credit: Shodan*

The second ShadowPad executable we found on VirusTotal targeted a computer in Russia that was operated by an organization involved with the distribution of public budgets. One submission was uploaded with a file name and the second submission was uploaded to

VirusTotal from China. The first file was submitted on November 3, 2017, and the second three days later on November 6, 2017.

In the second submission, we found a 7ZIP file that contained further files, including the previous submission, along with an encrypted log from the keylogger module. We decrypted the log file and found keypresses in various processes, such as from Microsoft Word, Firefox, Windows Explorer, and КриптоПро CSP (CryptoPro CSP). The most interesting were logs from Firefox, where the user completed financial transactions. We also found a contract, which is also public record, and names of employees involved in these processes.

An interesting takeaway from the analysis of the ShadowPad version from Russia was that ShadowPad hasn't always been modular. In the version from Russia, all modules were bundled in one executable, rather than separately stored in the Windows registry, as was the case with the version used for the Piriform attack. The bundled version gave us insights into a more thorough range of modules the attackers programmed. The attackers didn't even bother to download some of them to the Piriform network; only three of the plugins that were used in the attack in Russia were also used for the Piriform attack.

```
fncs.sub_10005DE0 = sub_10005DE0;
v1 = decrypt_string(8, "DISK", &out);
pluginfo(&a1->disk, v1->pwchar4, disk_init, disk_1_api, return_zero);
qstr::dtor(&out);
(a1->disk.init)(&fncs);
v2 = decrypt_string(8, "DISK", &out);
pluginfo(&a1->disk_2, v2->pwchar4, disk_2_init, disk_2_api, return_zero);
qstr::dtor(&out);
(a1->disk_2.init)(&fncs);
v3 = decrypt_string(13, "KeyLogger", &out);
pluginfo(&a1->keylogger, v3->pwchar4, keylogger_init, keylogger_api, keylogger_dtor);
qstr::dtor(&out);
(a1->keylogger.init)(&fncs);
v4 = decrypt_string(11, "Nethood", &out);
pluginfo(&a1->nethood, v4->pwchar4, Nethood_init, Nethood_api, return_zero);
qstr::dtor(&out);
(a1->nethood.init)(&fncs);
v5 = decrypt_string(11, "Netstat", &out);
pluginfo(&a1->netstat, v5->pwchar4, Netstat_init, Netstat_api, return_zero);
qstr::dtor(&out);
(a1->netstat.init)(&fncs);
v6 = decrypt_string(10, "Option", &out);
pluginfo(&a1->option, v6->pwchar4, Option_init, Option_api, return_zero);
qstr::dtor(&out);
(a1->option.init)(&fncs);
v7 = decrypt_string(11, "PortMap", &out);
pluginfo(&a1->portmap, v7->pwchar4, PortMap_init, PortMap_api, return_zero);
qstr::dtor(&out);
(a1->portmap.init)(&fncs);
v8 = decrypt_string(11, "Process", &out);
pluginfo(&a1->process, v8->pwchar4, Process_init, Process_api, return_zero);
qstr::dtor(&out);
(a1->process.init)(&fncs);
v9 = decrypt_string(11, "Regedit", &out);
pluginfo(&a1->regedit, v9->pwchar4, Regedit_init, Regedit_api, return_zero);
qstr::dtor(&out);
(a1->regedit.init)(&fncs);
v10 = decrypt_string(10, "Screen", &out);
pluginfo(&a1->screen, v10->pwchar4, Screen_init, Screen_api, Screen_dtor);
qstr::dtor(&out);
(a1->screen.init)(&fncs);
v11 = decrypt_string(11, "Service", &out);
pluginfo(&a1->service, v11->pwchar4, Service_init, Service_api, return_zero);
qstr::dtor(&out);
(a1->service.init)(&fncs);
v12 = decrypt_string(9, "Shell", &out);
pluginfo(&a1->shell, v12->pwchar4, Shell_init, Shell_api, return_zero);
qstr::dtor(&out);
(a1->shell.init)(&fncs);
v13 = decrypt_string(7, "SQL", &out);
pluginfo(&a1->sql, v13->pwchar4, SQL_init, SQL_api, return_zero);
qstr::dtor(&out);
(a1->sql.init)(&fncs);
v14 = decrypt_string(10, "Telnet", &out);
pluginfo(&a1->telnet, v14->pwchar4, Telnet_init, Telnet_api, return_zero);
qstr::dtor(&out);
(a1->telnet.init)(&fncs);
v15 = CreateEventW(0, 1, 0, 0);
a1->handle = v15;
if ( !v15 )
  return GetLastError();
v17 = new_plugin_record();
return spawn_thread(v17, &a1->handle_2, "PP", &loc_100071A3, a1);
```

ShadowPad modules used in the Russian attack

The oldest malicious executable used in the Russian attack was built in 2014, which means the group behind it might have been spying for years. The specific payment information we found traced by the key logger is public record, however it is likely that the attackers also accessed sensitive information.

Cybersecurity needs to become a core part of M&A due diligence

The examples of ShadowPad in South Korea and Russia re-emphasize that ShadowPad has been active for a long time, and it is frightening to see how ShadowPad can spy on institutions and organizations so thoroughly.

In terms of CCleaner, up to 2.27 million CCleaner consumers and businesses downloaded the infected CCleaner product. The attackers then installed the malicious second stage on just 40 PCs operated by high-tech and telecommunications companies. We don't have proof that a possible third stage with ShadowPad was distributed via CCleaner to any of the 40 PCs.

For Avast, there are two key takeaways from the CCleaner attack. First, M&A due diligence has to go beyond just legal and financial matters. Companies need to strongly focus on cybersecurity, and for us this has now become one of the key areas that require attention during an acquisition process. Second, the supply chain hasn't been a key priority for businesses, but this needs to change. Attackers will always try to find the weakest link, and if a product is downloaded by millions of users it is an attractive target for them. Companies need to increase their attention and investment in keeping the supply chain secure.