Endpoint Protection

View Only

Duuzer back door Trojan targets South Korea to take over computers

Oct 26, 2015 09:01 AM

A L Johnson

Symantec has found that South Korea is being impacted by an active back door Trojan, detected as Backdoor.Duuzer. While the malware attack has not been exclusively targeting the region, it has been focusing on the South Korean manufacturing industry. Duuzer is a well-designed threat that gives attackers remote access to the compromised computer, downloads additional files, and steals data. It's clearly the work of skilled attackers looking to obtain valuable information.

There is also evidence to suggest that the actors behind Duuzer are spreading two other threats, detected as W32.Brambul and Backdoor.Joanap, to target more organizations in South Korea. Brambul and Joanap appear to be used to download extra payloads and carry out reconnaissance on infected computers.

Duuzer: An advanced back door threat
Duuzer is an ongoing threat that is being delivered in targeted attacks. While the exact distribution method is unknown, it's likely that the malware is spreading through spear-phishing emails or watering-hole attacks.

The Trojan has been designed to work on both 32-bit and 64-bit computers. It also detects whether the computer it has infected is a virtual machine that was made using Virtual Box or VMware. If this is the case, then Duuzer stops executing. This allows Duuzer to attempt to evade detection from security researchers who are running virtual machines that are designed to be compromised with malware for analysis.

Once Duuzer infects a computer, it opens a back door, giving the attackers access to almost everything. The attackers can securely connect to the compromised computer through the threat and perform the following activities:

- Gather system and drive information
- Create, enumerate, and end processes
- Access, modify, and delete files
- Upload and download files
- Change the time attributes of files
- Execute commands

The Duuzer attackers have been observed trying to disguise their malware on an infected computer. They do this by identifying what software is installed and runs on startup, then renaming their malware to a similar title of an existing, legitimate program.

Based on our analysis of Duuzer, the attackers behind the threat appear to be experienced and have knowledge about security researchers' analysis techniques. Their motivation seems to be obtaining valuable information from their targets' computers.

The attackers appear to be manually running commands through the back door on affected computers. In one case, we observed the attackers creating a camouflaged version of their malware, and in another, we saw them attempting, but failing, to deactivate Symantec Endpoint Protection (SEP).

Duuzer in disguise
The attackers began by querying the Run key in the registry, redirecting the output to a temporary file:

- cmd.exe /c "reg query "HKLM\Software\Microsoft\Windows\CurrentVersion\Run" > C:\Windows\TEMP\BP25B4.tmp" 2>&1

They narrowed their query down to a specific user's Run key:

- cmd.exe /c "reg query "HKEY_USERS\[REMOVED]\Software\Microsoft\Windows\CurrentVersion\Run" > C:\Windows\TEMP\BP6380.tmp" 2>&1

The attackers discovered that a particular program was installed on the affected computer and decided to mimic that software. They created a new folder with the same name as the identified application, but in a different location. They then copied their malware into that folder:

- cmd.exe /c "md C:\USER_PROFILE\AppData\Local\[REMOVED]"

The attackers listed out the attributes for the file that they attempted to mimic. They then changed the attributes of their malicious file to match those of the clean one.

- cmd.exe /c "dir /a "C:\Program Files (x86)\[REMOVED]\[REMOVED] AGENT\[REMOVED].exe" > C:\Windows\TEMP\BPD0B6.tmp" 2>&1

Finally, the attackers created a new registry entry in the Run subkey to load their malware. Again, they used a similar name to the legitimate application to mimic it.

- cmd.exe /c "reg add "HKEY_USERS\[REMOVED]\Software\Microsoft\Windows\CurrentVersion\Run" /v "[REMOVED]Agent" /t REG_SZ /d "\"C:\USER_PROFILE\AppData\Local\[REMOVED]\[REMOVED].exe\"" /f > C:\Windows\TEMP\BPA62F.tmp" 2>&1

The attackers launched the camouflaged version of the malware, ended the old instance process, and deleted the first instance of the malware. At this point, having blended into the victim process, the attackers began to explore the local network using standard network enumeration tools.

Failing to deactivate Symantec Endpoint Protection
On a separate computer, during their network-mapping exercise, the attackers were unable to bypass SEP detections and attempted to disable the application. To do this, they installed an API-hooking tool in an effort to discover how the security application was interfacing with Windows and deactivate it. However, they were unable to stop SEP's monitoring activities.

The Brambul/Joanap connection
During our research, we found a dropper that infects computers with a worm known as Brambul and a back door Trojan called Joanap. It's unclear how the dropper is being distributed, but it's likely that it comes from malicious emails. Our analysis into Duuzer indicates that the Trojan is associated with both Brambul and Joanap. Computers infected with Brambul have been used as command-and-control (C&C) servers for Duuzer and have also been compromised with Duuzer.

The Brambul worm uses brute-force attacks to propagate. The threat connects to random IP addresses through the Server Message Block (SMB) protocol using a hardcoded list of user names and passwords. The passwords are quite common or easy to guess, such as "123123", "abc123", "computer," "iloveyou," "login", and "password".

After Brambul compromises a computer, it creates a net share to give attackers access to the system drive (usually the C: drive). It sends a message with the computer's details and login credentials to a hardcoded email address. Brambul's variants may be able to drop additional threats.

Joanap is dropped alongside Brambul and registers itself as a service with the display name "SmartCard Protector." This threat can open a back door, send specific files to the attackers, save or delete files, download and run executables, and launch or end processes.

Joanap also sends commands and configuration data over an RC4-encrypted connection to other computers infected with these threats. These commands could include running or ending processes, moving or deleting files, and updating C&C details.

Mitigation
Duuzer, Brambul, and Joanap are just a small selection of many threats affecting South Korea. The nation has been impacted in high-profile, targeted campaigns over the last few years. According to the region's National Computing & Information Agency (NCIA), there have been more than 114,035 attacks targeting government agencies between 2011 and 2015 so far. The numerous malicious campaigns in the region highlight how attackers continue to see South Korea as an attractive target.

Symantec recommends that users and businesses adhere to the following best practices to prevent their computers from being compromised with this malware:

- Change default user names and passwords
- Avoid using common or easy-to-guess passwords. The Norton Security Center has advice on how to pick strong passwords.
- Ensure that the operating system and software is regularly updated to prevent known vulnerabilities from being exploited
- Don't open suspicious emails. These messages typically distribute malware through malicious links and attachments.
- Keep security software up-to-date with the latest definitions

Protection
Norton Security, Symantec Endpoint Protection, and other Symantec security products protect users against these threats through the following detections:

Antivirus

- Backdoor.Duuzer
- W32.Brambul
- Backdoor.Joanap

Intrusion Prevention System

- System Infected: Backdoor.Joanap Activity

We've also provided the indicators of compromise for Duuzer, Brambul, and Joanap, as follows:

Backdoor.Duuzer indicators of compromise
MD5

- 1205c4bd5d02782cc4e66dfa3fef749c
- 92d618db54690c6ae193f07a31d92098
- 3e6be312a28b2633c8849d3e95e487b5
- 41a6d7c944bd84329bd31bb07f83150a
- 7343f81a0e42ebf283415da7b3da253f
- 73471f41319468ab207b8d5b33b0b4be
- 84a3f8941bb4bf15ba28090f8bc0faec
- b04fabf3a7a710aafe5bc2d899c0fc2b
- e04792e8e0959e66499bfacb2a76802b
- 3a963e1de08c9920c1dfe923bd4594ff
- 51b3e2c7a8ad29f296365972c8452621
- 5f05a8f1e545457dbd42fe1329f79452
- 91e5a64826f75f74a5ae123abdf7cef5
- 9749a4b538022e2602945523192964ad
- 9ca7ec51a98c2b16fd7d9a985877a4ba
- bb6cbebd4ffd642d437afc605c32eca0
- fb4caaaf1ac1df378d05111d810a833e
- 4b2d221deb0c8042780376cb565532f8
- cd7a72be9c16c2ece1140bc461d6226d
- f032712aa20da98a1bbad7ae5d998767
- f940a21971820a2fcf8433c28be1e967
- 71cdcc903f94f56c758121d0b442690f
- 0f844300318446a70c022f9487475490

SHA256

- fd5a7e54cfdd3b3f32b44d8fdd845e62d6b86c0ddb550c544d659588d06ceaee
- 89b25f9a454240a3f52de9bf6f9a829d2b4af04a7d9e9f4136f920f7e372909b
- a01bd92c02c9ef7c4785d8bf61ecff734e990b255bba8e22d4513f35f370fd14
- c327de2239034b6f6978884b33582ce97761bcc224239c955f62feebd01e5946
- c7024cf43d285ec9671e8dc1eae87281a6ee6f28e92d69d94474efc2521f03ed
- 5a69bce8196b048f8b98f48c8f4950c8b059c43577e35d4af5f26c624140377c
- 477ca3e7353938f75032d04e232eb2c298f06f95328bca1a34fce1d8c9d12023
- d57d772eefa6086b5c249efff01189cf4869c2b73007af63affc353474eaafcb
- 4efeea9eeae3d668897206eeccb1444d542ea537ca5c2787f13dd5dadd0e6aaa
- a0a6d0e3af6e76264db1e0d4a4ad5745fff15eb2790938718b2c0988b9415b2b
- 5b28c86d7e581e52328942b35ece0d0875585fbb4e29378666d1af5be7f56b46
- 47181c973a8a69740b710a420ea8f6bf82ce8a613134a8b080b64ce26bb5db93
- fb6d81f4165b41febc739358aeba0fe15048e1d445296e8df9104875be30f9a7
- 4a6aba1c182dd8304bac91cc9e1fc39291d78044995f559c1d3bce05afd19982

- 7099093177094ea5cc3380b42c2556ed6e8dd06a2f537fa6dd275e5cc1df9c9a
- 90d8643e7e52f095ed59ed739167421e45958984c4c9186c4a025e2fd2be668b
- 66df7660ddae300b1fcf1098b698868dd6f52db5fcf679fc37a396d28613e66b
- 37f652e2060066a1c2c317195573a334416f5a9b9933cfb1ece55bea8048d80f
- 6b71465e59eb1e266d47efeaecc256a186d3e08f570bffcfd5ac55e635c67c2a
- d2e03115ef1525f82d70fc691f0360e318ade176a3789cf36969630d9af6901a
- 912905ec9d839ca8dfd6771ff5c17aec3516f9ad159a9d627b81261055095fbf
- 4cf3a7e17dc4628725dd34b8e98238ed0a2df2dc83189db98d85a38f73706fa5

W32.Brambul indicators of compromise
MD5

- 1c532fad2c60636654d4c778cfe10408
- 1db2dced6dfa04ed75b246ff2784046a
- 3844ec6ec70347913bd1156f8cd159b8
- 40878869de3fc5f23e14bc3f76541263
- 95a5f91931723a65dcd4a3937546da34
- 99d9f156c73bd69d5df1a1fe1b08c544
- a1ad82988af5d5b2c4003c42a81dda17
- ca4c2009bf7ff17d556cc095a4ce06dd
- f273d1283364625f986050bdf7dec8bb

SHA256

- c029ae20c314d7a0a2618f38ced03bac99e2ff78a85fe8c8f8de8555a8d153ab
- 1da344e5e55bef4307e257edd6f1e14835bdae17538a74afa5fc12c276666112
- 9c3e13e93f68970f2844fb8f1f87506f4aa6e87918449e75a63c1126a240c70e
- 230c2727e26467e16b5cf3ca37ecb8436ee5df41bfc4cd04062396642f9de352
- d558bb63ed9f613d51badd8fea7e8ea5921a9e31925cd163ec0412e0d999df58
- cbb174815739c679f694e16484a65aa087019272f94bcbf086a92817b4e4154b
- 61f46b86741c95336cdac3f07f42b7df3e84695968534be193e98ea76d1070d1
- 1dea57b33a48c79743481371a19e17f68ae768a26abc352f21560308698c786f
- 8df658cba8f8cf0e2b85007f57d79286eec6309e7a0955dd48bcd15c583a9650

Backdoor.Joanap indicators of compromise
MD5

- fd59af723b7a4044ab41f1b2a33350d6
- 4613f51087f01715bf9132c704aea2c2
- 074dc6c0fa12cadbc016b8b5b5b7b7c5
- 27a3498690d6e86f45229acd2ebc0510
- 7a83c6cd46984a84c40d77e9acff28bc
- 1d8f0e2375f6bc1e045fa2f25cd4f7e0
- 304cea78b53d8baaa2748c7b0bce5dd0
- a1ad82988af5d5b2c4003c42a81dda17

SHA256

- 9a179e1ca07c1f16c4c1c4ee517322d390cbab34b5d123a876b38d08da1face4
- a1c483b0ee740291b91b11e18dd05f0a460127acfc19d47b446d11cd0e26d717
- 7650d8c0874aa7d1f2a5a7d255112976e9f38ffad8b7cdda76d0baa8f4729203
- 5b10cfb236d56a0f3ddaa5e9463ebf307b1d2e0624b0f1c6ece19213804b6826
- 0622481f1c1e246289014e9fe3497e69f06ed8b3a327eda86e4442a46790dd2e
- 4c5b8c3e0369eb738686c8a111dfe460e26eb3700837c941ea2e9afd3255981e
- cbf5f579ff16206b17f039c2dc0fa35704ec01ede4ba18ecb1fc2c7b8217e54f
- 61f46b86741c95336cdac3f07f42b7df3e84695968534be193e98ea76d1070d1

Tags and Keywords

Related Entries and Links

No Related Resource entered.

PRODUCTS APPLICATIONS SUPPORT COMPANY HOW TO BUY