Four Years of DarkSeoul Cyberattacks Against South Korea Continue on Anniversary of Korean War

web.archive.org/web/20130701021735/https://www.symantec.com/connect/blogs/four-years-darkseoul-cyberattacks-against-south-korea-continue-anniversary-korean-war

Created: 26 Jun 2013 22:33:21 GMT | Updated: 27 Jun 2013 12:21:33 GMT | Translations available: 日本語

Symantec Security Response Symantec Employee
+2 2 Votes
Login to vote

Tweet

Yesterday, June 25, the Korean peninsula observed a series of cyberattacks coinciding with the 63rd anniversary of the start of the Korean War. While multiple attacks were conducted by multiple perpetrators, one of the distributed denial-of-service (DDoS) attacks observed yesterday against South Korean government websites can be directly linked to the DarkSeoul gang and Trojan.Castov.

We can now attribute multiple previous high-profile attacks to the DarkSeoul gang over the last 4 years against South Korea, in addition to yesterday's attack. These attacks include the devastating Jokra attacks in March 2013 that wiped numerous computer hard drives at South Korean banks and television broadcasters, as well as the attacks on South Korean financial companies in May 2013.

Conducting DDoS attacks and hard disk wiping on key historical dates is not new for the DarkSeoul gang. They previously conducted DDoS and wiping attacks on the United States Independence Day as well.

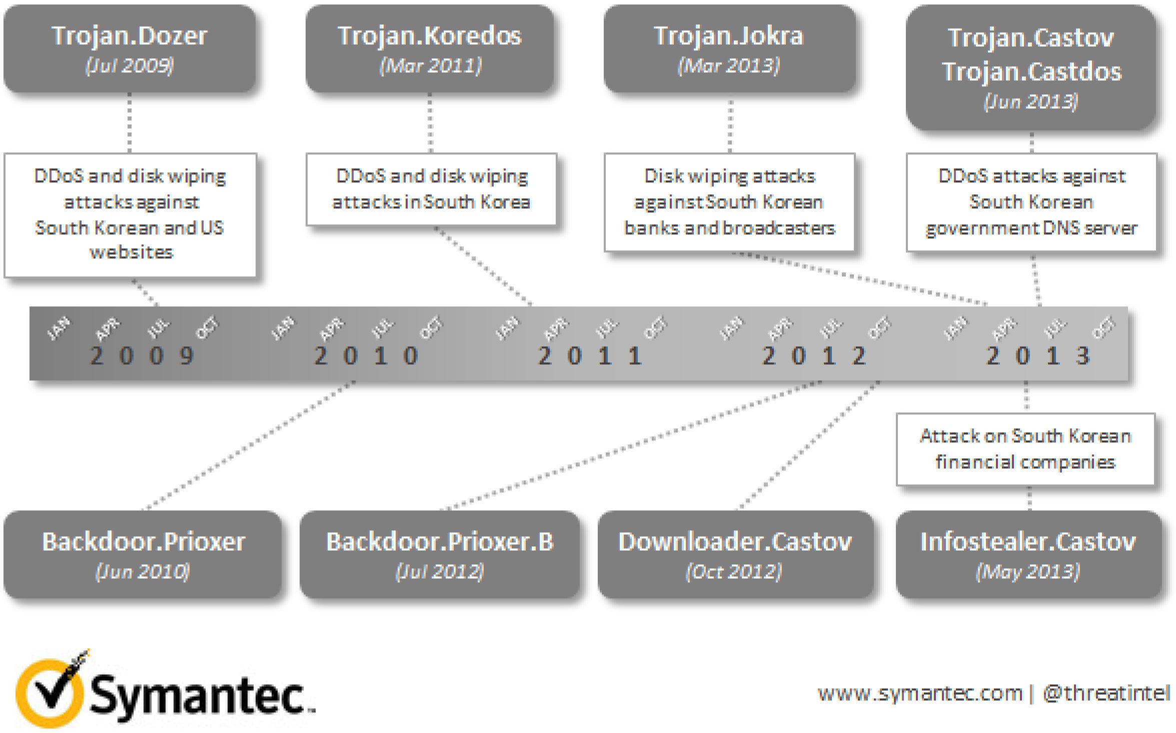
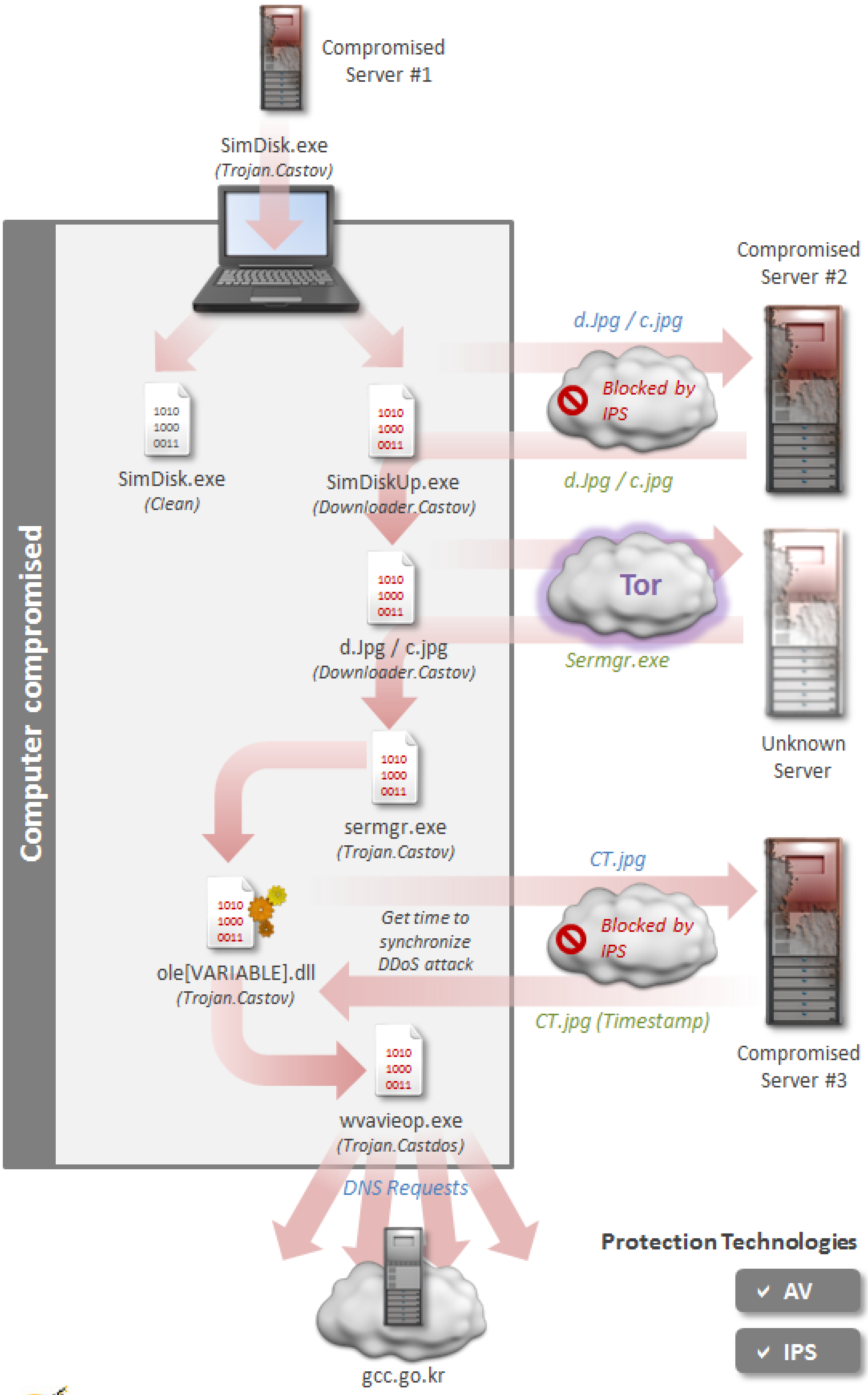

Trojan.Dozer
(Jul 2009)
Trojan.Koredos
(Mar 2011)
Trojan.Jokra
(Mar 2013)
Trojan.Castov
Trojan.Castdos
(Jun 2013)
DDoS and disk wiping attacks against South Korean and US websites
DDoS and disk wiping attacks in South Korea
Disk wiping attacks against South Korean banks and broadcasters
DDoS attacks against South Korean government DNS server
JAN APR JUL OCT
2009
2010
2011
2012
2013
Attack on South Korean financial companies
Backdoor.Prioxer
(Jun 2010)
Backdoor.Prioxer.B
(Jul 2012)
Downloader.Castov
(Oct 2012)
Infostealer.Castov
(May 2013)
Symantec.
www.symantec.com | @threatintel

Figure 1. *Four years of DarkSeoul activity*

The DarkSeoul gang's attacks tend to follow similar methods of operation. Trademarks of their attacks include:

- Multi-staged, coordinated attacks against high-profile targets in South Korea
- Destructive payloads, such as hard disk wiping and DDoS attacks configured to trigger on historically significant dates
- Overwriting disk sectors with politically-themed strings
- Use of legitimate third-party patching mechanisms in order to spread across corporate networks
- Specific encryption and obfuscation methods
- Use of specific third-party webmailer servers to store files
- Use of similar command-and-control structures

The attacks conducted by the DarkSeoul gang have required intelligence and coordination, and in some cases have demonstrated technical sophistication. While nation-state attribution is difficult, South Korean media reports have pointed to an investigation which concluded the attackers were working on behalf of North Korea. Symantec expects the DarkSeoul attacks to continue and, regardless of whether the gang is working on behalf of North Korea or not, the attacks are both politically motivated and have the necessary financial support to continue acts of cybersabotage on organizations in South Korea. Cybersabotage attacks on a national scale have been rare—Stuxnet and Shamoon (W32.Disttrack) are the other two main examples. However, the DarkSeoul gang is almost unique in its ability to carry out such high-profile and damaging attacks over several years.


Compromised Server #1
SimDisk.exe
(Trojan.Castov)
Computer compromised
SimDisk.exe
(Clean)
SimDiskUp.exe
(Downloader.Castov)
Compromised Server #2
d.Jpg / c.jpg
Blocked by IPS
d.Jpg / c.jpg
d.Jpg / c.jpg
(Downloader.Castov)
Tor
Sermgr.exe
Unknown Server
sermgr.exe
(Trojan.Castov)
CT.jpg
Get time to synchronize DDoS attack
Blocked by IPS
CT.jpg (Timestamp)
Compromised Server #3
ole[VARIABLE].dll
(Trojan.Castov)
wvavieop.exe
(Trojan.Castdos)
DNS Requests
gcc.go.kr
Protection Technologies
✓ AV
✓ IPS

Symantec.

Figure 2. *Castov DDoS attack*

The Castov DDoS attack occurs in the following manner:

1. Compromised website leads to the download of SimDisk.exe (Trojan.Castov), a Trojanized version of a legitimate application.
2. SimDisk.exe drops two files onto the compromised system: SimDisk.exe (Clean), the legitimate non-Trojanized version, and SimDiskup.exe (Downloader.Castov).
3. Downloader.Castov connects to a second compromised server to download the C.jpg file (Downloader.Castov), an executable file which appears to be an image.
4. Threat uses the Tor network to download Sermgr.exe (Trojan.Castov).
5. Castov drops the Ole[VARIABLE].dll file (Trojan.Castov) in the Windows system folder.
6. Castov downloads the CT.jpg file from a Web server hosting a ICEWARP webmail, that has been compromised as a result of publicly known vulnerabilities in ICEWARP. The CT.jpg file contains a timestamp used by Castov to synchronize attacks.
7. Once this time is reached, Castov drops Wuauieop.exe (Trojan.Castdos).
8. Castdos begins to overload the Gcc.go.kr DNS server with DNS requests, effectively performing a DDoS attack affecting multiple websites.

Blog Entry Filed Under: