Dark South Korea Total War Review

eromang.zataz.com/tag/agentbase-exe/

02/04/2013

As mentioned by different medias, security vendors and security researchers some South Korean banks and broadcasting organizations went dark Wednesday 20 March, victim of a cyber attack. Initial impacted broadcaster were **KBS**, **MBC** and **YTN**, and impacted banks were **Cheju**, **Nonghyup** and **Shinhan**.

But by analyzing all the events related to this cyber attack we can see that the campaign was more extended in time as mentioned and also more complex to understand. The campaign is composed by different samples, created potentially by different authors with different objectives. We can divide the reported samples in different categories:

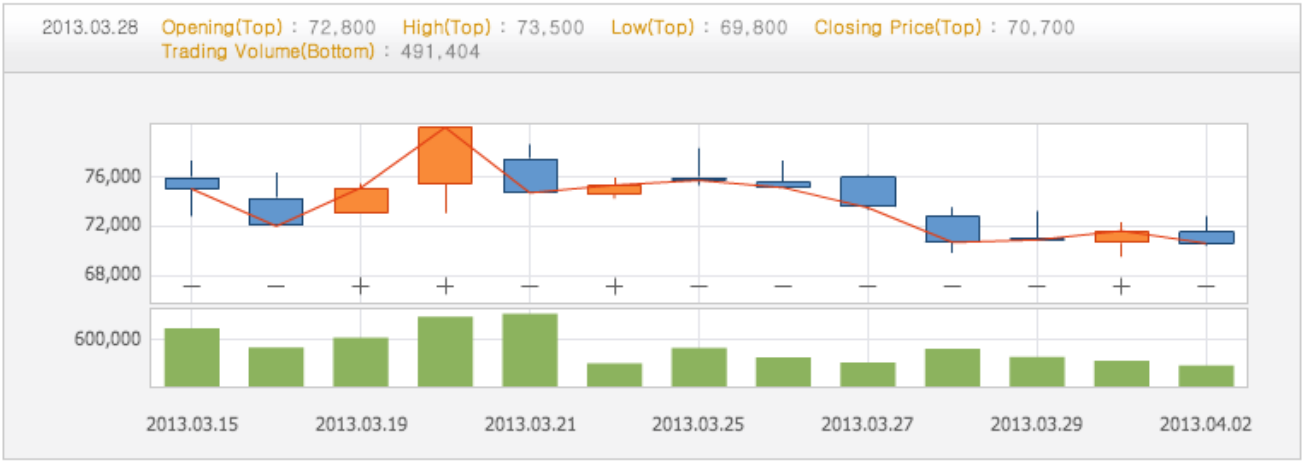
- **Wipe**: Objective of these samples is to erase all data's of affected targets.
- **Drop & Wipe**: Objective of these samples is to drop a wiper to erase all data's of affected targets.
- **Drop & Wipe & Deface**: Objectives of these samples are to drop a wiper to erase all data's and deface website hosted by affected targets.
- **Drop & Backdoor**: Objective of these samples is to install a backdoor, or trojan, on the affected targets.
- **Unknown**: These samples are potentially not related to the campaign.

I will try, through this blog post, to provide you the most reliable information's as possible regarding the Dark South Korea campaign.

According to different sources, and announced by the South Korean security provider **AhnLab** the Thursday 21 March, "*bad guys*" got access to *AhnLab Policy Center* and *HAURI ViRobot ISMS*, asset management tools, through stolen credentials in order to massively spread **Trojan.Jokra**. But, regarding the latest news announced the 29 March, it

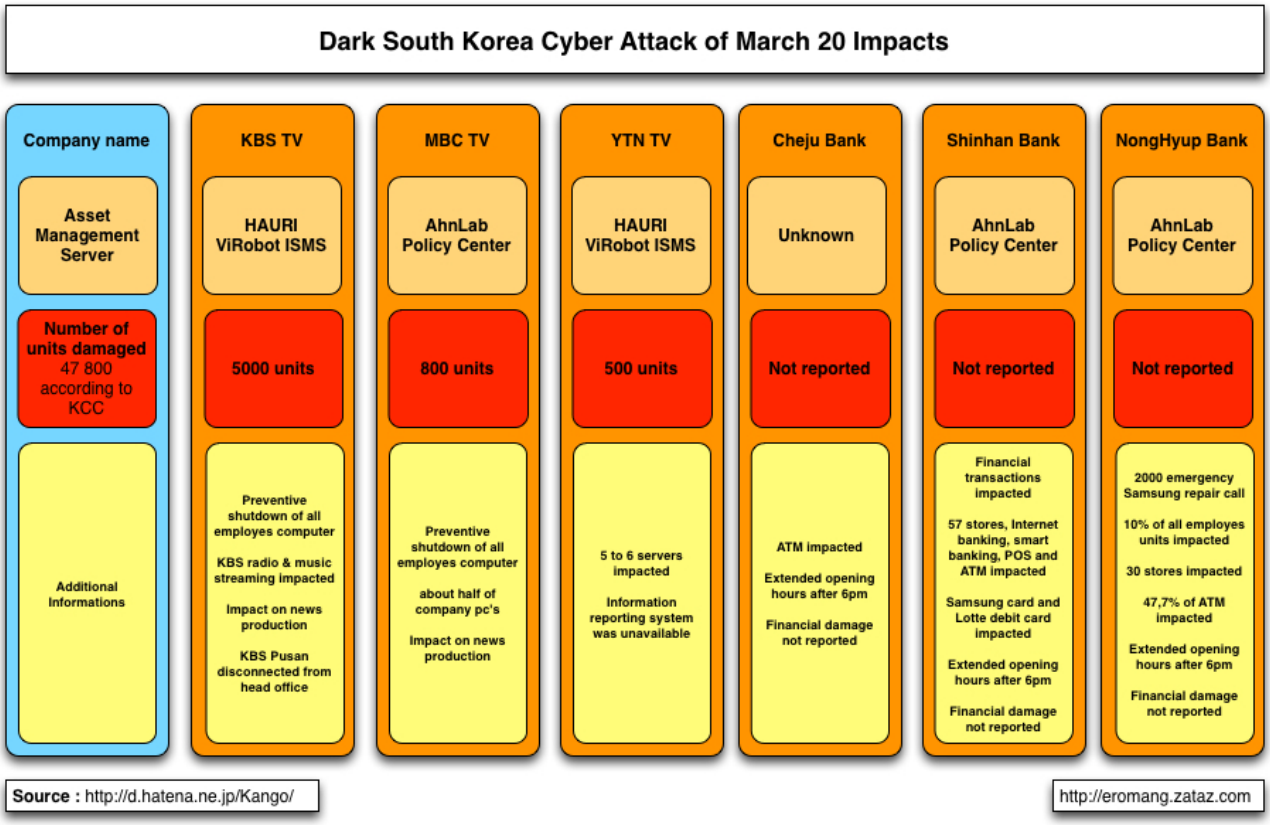
seem that AhnLab APC product was vulnerable to a login authentication bypass and that this vulnerability was used by the bad guys in order to get access to APC and spread the malware.

On Wednesday 20 March, AhnLab stocks gains of 6.5 percent (75,100 KW to 80,000 KW) from stemming from expectations of demand for online security software following the hacking incident. But after the 21 March AhnLab announcement, stocks were down 3.6 percent (from 80,000 KW to 74,700 KW). Since 21 March, AhnLab stocks have fallen from 74,700 KW to 68,100 KW.



AhnLab Stocks. Source: Korea Exchange

KCC reported that around 47 800 units were impacted by this cyber attack. You will find in the following graphical representation of known impacts. This graphical representation has been inspired by the work of **@piyokango**, a must **read blog post** !



Also translated from **@piyokango** work, the associated event timeline. Through this timeline you can better understand all the actors and impacts involved in this cyber attack.

Dark South Korea Events Timeline

Date	Time	Event
3/20	At around 2pm	Financial and broadcasting organizations computers stop suddenly and cannot restart
2:25pm	KCC start to receive incident reports	
2:35pm	KCC & KISA confirm outages on financial and broadcasting organizations	
2:40pm	YTN TV report the incidents	
2:50pm	South Korea presidence acknowlege the incidents	
3pm	KISA raise his alert level	
Date	**Time**	**Event**

Date	Time	Event
3:05pm	NongHyup Bank initiate blocking measures	
At around 3pm	Shinhan bank central server is down	
At around 3pm	Cyber police announce the possibility of an attack and start the investigation	
3:10pm	South Korean army raise his alert level	
3:20pm	Shinhan bank business recovery	
4:20pm	NongHyup bank business recovery	
At around 4pm	MBC TV internal network reported as impacted	
At around 4pm	Extended opening hours after 6pm for banks	
5:49pm	AhnLab anti-virus engine is updated	
6:40pm	AhnLab distribute counter measures	
At around 9pm	KBS internal information system reported as impacted	
3/21	6:30am	MBC Gyeongnam TV internal network is stopped
7:25am	KBS TV internal network business recovery, except for PC's	
11:30am	KCC chairman visit KISA	
At around 5pm	16 NongHyup bank offices still not able to recover	
3/22	At around 6am	87% of NongHyup bank cooperatives and 78% of they're ATM's have been recovered
At around 3pm	KCC report that China attribution was a mistake.	
3/24	At around 6pm	NongHyup bank add some additional counter measures

Date	Time	Event

Date	Time	Event
NongHyup bank full business recovery		
3/25	At around 6am	NongHyup bank segregate internal and external network (lol)
10:30am to 1:45pm	Time zone attacks reported and security warning raised by AnhLab	
International cooperation requested for investigations		
3/26	9:21am	Additional counter measures provided by AhnLab
9:40am	6 YTN TV affiliates overloaded by traffic	
10:40am	Network overload disrupting 8 municipalities web sites (Seoul, Gyeonggi, Incheon, Gwangju, Jeonnam, Jeonbuk, Gangwon, Jeju).	
11:22am	Network overload disrupting 7 South Korean regions.	
11:50am	Military experts join the public-private incident response task force	
00:04pm	Network failure recovery	
01:40pm to 02:30pm	Daily NK web site disrupted and posts deleted	
Free North Korea TV web site disrupted		
02:00pm to 02:15pm	Ministries web site disrupted	
02:30pm to around 05pm	Other North Korean activists web sites disrupted	

Date	Time	Event

Date	Time	Event
3/27	-	The Financial Services Commission announce special inspections on targeted financial institutions
3/28	-	YTN TV web site recovery
3/29	11:09am	AhnLab announce that APC was vulnerable to a authentication bypass weakness
-	Response Team announce return to normalization	

Date	Time	Event

Source : piyolog (http://d.hatena.ne.jp/Kango/20130323)
The actual investigation results point that foreign source IPs (3 european countries and US, but not China) were discovered as potential source of the attack, and that a potential of 14 variants of the malware were discovered and analyzed.

Security firm **Xecure Lab** has provide some information's regarding Dark South Korea, malwares hash are available with some detailed analysis. Also malwares samples were available on private groups and on **contagio**. Based on these hashes and samples, you can find here under an analysis.

Samples Analysis

Presumed Dropper(s)

MD5	9263E40D9823AECF9388B64DE34EAE54
Size	417.5 KB
Compilation timedatestamp	2013-03-20 04:07:02
Modify Date	None
File mapping object	None
Resource language(s)	English & Korean
Strings	N/A
URL	None
Other names	APCRunCmd.DRP - K10

This executable drop "*AgentBase.exe*" (db4bbdc36a78a8807ad9b15a562515c4), "*alg.exe*" (e45cd9052dd3dd502685dfd9aa2575ca), "*conime.exe*" (6a702342e8d9911bde134129542a045b) and "*~pr1.tmp*" (dc789dee20087c5e1552804492b042cd) in "*%TMP%*", then execute "*AgentBase.exe*". Remarks: Also known as K10 by Xecure Lab, mentioned as a wiper, but it is a dropper. This sample could be categorized as **Drop & Wipe**.

Also, dropped "*AgentBase.exe*" is known as K01 on Xecure Lab, mentioned as a wiper only. "*AgentBase.exe*" is a Windows wiper, but also the dropper for *NIX batch wiper aka "*~pr1.tmp*". More information's in the "*9263E40D9823AECF9388B64DE34EAE54 Dropper Analysis*" chapter of this blog.

MD5	50E03200C3A0BECBF33B3788DAC8CD46
Size	24 KB
Compilation timedatestamp	2012-07-06 12:24:18
Modify Date	None
File mapping object	FFFFFFF-198468CD-6937629023-EF90000000
Resource language(s)	None
Strings	hello
URL	hxxp://www.skymom.co.kr/rgboard/addon/update/update_body.jpg
Other names	K06

It seem that "*update_body.jpg*" (a03ae3a480dd17134b04dbc5e62bf57b), first seen the 2012-08-28 04:31:52, is the same as mentioned on **SCUMWARE** the 2012-08-30. You can find this sample on **malware.lu**. **Symantec** and **McAfee** have try to create a relation based on the used packer and on some common compilation paths. But like McAfee, I don't see any relations between this dropper and the 03.20 Dark South Korea campaign. Known as K06 on Xecure Lab. This sample could be categorized as **Drop & Backdoor**, or **Unknown**.

MD5	E4F66C3CD27B97649976F6F0DAAD9032
Size	24 KB
Compilation timedatestamp	2012-07-06 12:24:18
Modify Date	None

File mapping object	FFFFFFF-198468CD-6937629023-EF90000000
Resource language(s)	None
Strings	hello
URL	hxxp://www.anulaibar.com/e107/e107_files/js/e107_001.cab
Other names	K05

Here also, I don't see any relations between this dropper and the 03.20 Dark South Korea campaign. Known as K05 on Xecure Lab and mentioned by McAfee. This sample could be categorized as **Drop & Backdoor**, or **Unknown.**

MD5	2F9AF723E807FF44C2684E5D644EBE46
Size	38.8 KB
Compilation timedatestamp	None
Modify Date	2013:03:17 23:41:07
File mapping object	None
Resource language(s)	None
Strings	None
URL	None
Other names	고객계좌내역.rar - K08

Known as K08 on xsecure-lab.com, and like the guys of Xecure Lab. I don't see any relations between this dropper and the 03.20 Dark South Korea campaign. **F-Secure** has try to link this sample to the campaign. This sample could be categorized as **Unknown**.

MD5	530c95eccdbd1416bf2655412e3dddb
Size	Unknown
Compilation timedatestamp	Unknown
Modify Date	None
File mapping object	Unknown
Resource language(s)	Unknown
Strings	HASTATI. / PR!NCPES and other unknowns

URL	Unknown
Other names	Unknown

This sample was mentioned by Symantec and AhnLab the 23 March. Particularities of this sample is that he will drop 2 files and inject 1 the files into "*LSASS.exe*" process as a DLL. Also this sample will be executed any years the 20 March at 2pm and wipe MBR with "HASTATI." and "PR!NCPES" strings. Unfortunately I wasn't able to find this sample. This sample could be categorized as **Drop & Wipe**.

MD5	e823221609b37e99fbbce5b493a02f68
Size	236.0 KB
Compilation timedatestamp	2013-03-19 23:57:06
Modify Date	None
File mapping object	None
Resource language(s)	Korean
Strings	MICRO_ESENCIAL0192301 / Alerter / Sens / Hacked By Whois Team / morpsntls.exe / and bunch of others
URL	None
Other names	cmsvrts.exe / K07

This sample was also mentioned the 20 March by different medias, security vendors and researchers. He was used to against LG UPlus Corp showed a page that said it had been hacked by a group calling itself the "*Whois Team*".

Particularities of this sample is that he seem to be triggered only in certain conditions, and this condition seem to be related to certain time zone, as mentioned by AhnLab the 23 March. The sample drop "*mp.swf*", "*lf.mp3*", "*24mhk04.gif*", "*25z18pg.jpg*" files, adds "*MICRO_ESENCIAL0192301*" as mutex, modify the "*SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management*" following registry entries, overwrite all "*.html*", "*.htm*", "*.aspx*", "*.asp*", "*.jsp*", "*.do*", "*.php*" files with its code, terminate Windows Alerter service (*Alerter*) and Windows System Event Notification Service (*Sens*), and drop all the MBR datas. This sample could be categorized as **Drop & Wipe & Deface**.

Presumed Wiper(s)

Symantec, **Tripwire**, Xecure Lab and contagio reported hashes of different wipers. Here under an analysis of these wipers with some corrections.

MD5	0a8032cd6b4a710b1771a080fa09fb87
Size	24 KB

Compilation timedatestamp	2013-01-31 10:27:18
File mapping object	JO840112-CRAS8468-11150923-PCI8273V
Strings	PR!NCPES / HASTATI. / \Temp\~v3.log
Check "~v3.log"	No
Task kill	pasvc.exe (AhnLab Policy Agent) / clisvc.exe (Hauri ViRobot)
Wiper timing	Immediate
Shutdown	shutdown -r -t 0
Other names	mb_join.gif / mb_join.exe / K03
Mentioned by	contagio & Symantec

Despite file "*~v3.log*" is present in "*C:\WINDOWS\Temp*" directory, the wiper is running directly. This sample could be categorized as **Wiper**.

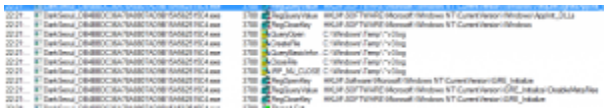
MD5	5fcd6e1dace6b0599429d913850f0364
Size	24 KB
Compilation timedatestamp	2013-01-31 10:27:18
File mapping object	JO840112-CRAS8468-11150923-PCI8273V
Strings	HASTATI.
Check "~v3.log"	No
Task kill	pasvc.exe (AhnLab Policy Agent) / Clisvc.exe (Hauri ViRobot)
Wiper timing	Immediate
Shutdown	shutdown -r -t 0
Other names	AmAgent.exe / OthDown.exe / K04
Mentioned by	contagio & Symantec & Tripwire

This sample could be categorized as **Wiper**.

MD5	db4bbdc36a78a8807ad9b15a562515c4

Size	24 KB
Compilation timedatestamp	2013-01-31 10:27:18
File mapping object	JO840112-CRAS8468-11150923-PCI8273V
Strings	PRINCPES / HASTATI. / \Temp\~v3.log
Check "~v3.log"	Yes
Task kill	pasvc.exe (AhnLab Policy Agent) / clisvc.exe (Hauri ViRobot)
Wiper timing	Not immediate if ~v3.log is present
Shutdown	shutdown -r -t 0
Other names	ApcRunCmd.exe / K01
Mentioned by	contagio & Symantec & Tripwire

This sample is taking care of the "*~v3.log*" presence in "*C:\WINDOWS\Temp*" directory. If the file is present the wipe process is not started. This sample could be categorized as **Wiper**.



But you have to take in consideration that this sample is normally executed by 9263E40D9823AECF9388B64DE34EAE54 dropper, and that a complete process will be analyzed in the "*9263E40D9823AECF9388B64DE34EAE54 Dropper Analysis*" chapter of this blog.

MD5	f0e045210e3258dad91d7b6b4d64e7f3
Size	24 KB
Compilation timedatestamp	2013-01-31 10:27:18
File mapping object	JO840112-CRAS8468-11150923-PCI8273V
Strings	PRINCPES / HASTATI. / \Temp\~v3.log
Check "~v3.log"	Yes
Task kill	pasvc.exe (AhnLab Policy Agent) / clisvc.exe (Hauri ViRobot)

Wiper timing	Not immediate if ~v3.log is present
Shutdown	shutdown -r -t 0
Other names	ApcRunCmd.exe / K02
Mentioned by	contagio

Like the previous wiper, if "*~v3.log*" is present in "*C:\WINDOWS\Temp*" directory, the wipe process is not started.

This sample seems also to be part of a another dropper actually not publicly known. This sample could be categorized as **Wiper**.

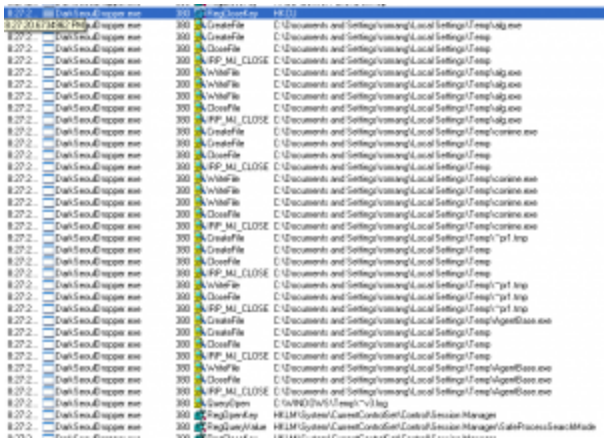
As you can see, all of the wipers use the "*HASTATI*" string in order to overwrite MBR data's. As reported by security vendors, "*Hastati*" term refers to a class of infantry in the armies of the early Roman Republic. "*PRINCPES*" term, also used to overwrite MBR data's, could also refer to the "*Principes*" who were veteran soldiers of the Roman Pre-Marian Army. Are the "*bad guys*" fan of Roman Army, or fan of **Total War** game ?

Also an interesting relation between the "*HASTATI*" string used to overwrite MBR data's, is that KBS TV website was defaced the 21 March with a "*Defaced by HASTATI*" message and symbol representing the class of infantry in the armies of the early Roman Republic.

9263E40D9823AECF9388B64DE34EAE54 Dropper Analysis

In this chapter of this long blog post we will analyze some behaviors of *9263e40d9823aecf9388b64de34eae54* dropper.

As mentioned by different security vendors or researchers, when executed the dropper will extract 4 files into Windows "*%TMP%*" directory. These files are "*alg.exe*", "*conime.exe*", "*~pr1.tmp*" and "*AgentBase.exe*".



"*alg.exe*" (*e45cd9052dd3dd502685dfd9aa2575ca*) is the "*plink.exe*" PuTTY tool acting as a command-line interface to the PuTTY back ends. This binary has been compiled the 2013-02-15 at 08:12:58.

"*conime.exe*" (6a702342e8d9911bde134129542a045b) is the "*pscp.exe*" PuTTY tool acting as a SCP client, i.e. command-line secure file copy. This binary has been compiled the 2006-03-13 at 14:32:44.

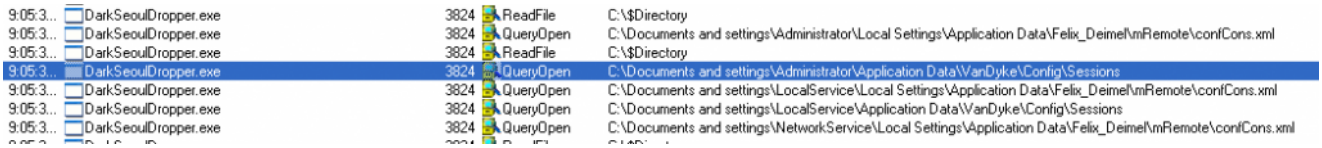
"*~pr1.tmp"* (*dc789dee20087c5e1552804492b042cd*) is a bash script who will be dropped and executed on *NIX servers in certain conditions.

"*AgentBase.exe*" (db4bbdc36a78a8807ad9b15a562515c4) is the wiper mentioned in the previous chapters of this blog post.

After installing these files, the dropper will check the presence of "*~v3.log*" file in "*C:\WINDOWS\Temp*" directory.

If the file "*~v3.log*" is not existing "*AgentBase.exe*" wiper will be executed, killing AhnLab Policy Agent (*pasvc.exe*) and Hauri ViRobot ISMS Client (*clisvc.exe*), then erasing all data's.

If the file "*~v3.log*" is existing, the dropper start to check the presence of configuration file "*confCons.xml*" of **mRemote** program, developed by Felix Deimel, and the presence of configuration files of **SecureCRT** program, developed by VanDyke Software, Inc.



For **mRemote**, the dropper copy all data's, related to SSH connexions with root login, present in "*confCons.xml*" configuration file and exploit a vulnerability present in the password storage engine of this program. When you save connections in mRemote it outputs all of that data into an XML report "*confCons.xml*". The passwords are saved in an encrypted format, however this is trivial to circumvent. So despite the passwords are saved in encrypted format it is easy to decrypt them. This vulnerability was discovered and published by **Cosine Security** the 2 Jun 2011. Support of mRemote has been stopped in 2012.

Once the mRemote vulnerability is exploited, the dropper start a new process to execute "*conime.exe*" binary, in order to drop the "*~pr1.tmp*" file into "*/tmp/cups*" on the targeted server:

"*C:\Users\ERICRO~1\AppData\Local\Temp\conime.exe -batch -P 22 -l root -pw test C:\Users\ERICRO~1\AppData\Local\Temp\~pr1.tmp 192.168.178.54:/tmp/cups*"

After upload of "*cups*" file, the dropper will execute this file through the following command.

"*C:\Users\ERICRO~1\AppData\Local\Temp\conime.exe -batch -P 22 -l root -pw test 192.168.178.54 "chmod 755 /tmp/cups;/tmp/cups*"

For **SecureCRT**, the dropper is also copying all data's, related to SSH connexions with root login, present in "**.ini*" configuration files. Each saved connection in SecureCRT as it ones "*.ini" file who will be parsed by the dropper. The passwords are also saved in an encrypted format.

With the latest version of SecureCRT (7.0.3), the dropper is unable to decrypt the password, but will try to connect to targeted servers with a wrong password. So there is surely a similar vulnerability as for mRemote in previous versions of SecureCRT, but wasn't able to find it.