UPD. Explanation of changing the modes of operation of the sample depending on the privileges received and the running processes

Due to the confusion that emerged regarding the modes of sample's operation, depending on the privileges received and the detected processes of antivirus products, a more detailed explanation is needed.

The sample does not stop its work when it detects the previously mentioned processes - but changes part of its functionality. If the "avp.exe" process is detected, the sample will not write MBR with MFT encryption, but will write zeros to the first sector of the disk - So that computer will not be able to boot after reboot – however it will not display screen with the demand for redemption; If the processes "ccSvcHst.exe" or "NS.exe" are found, the sample will not exploit SMB, but will run mimikatz, and use the received data for propagation attempts via PsExec / wmic.

Mask of privileges		
Bit 1	Bit 2	Bit 3
1 if there is a SeShutdownPrivilege Otherwise 0	1 if there is a SeDebugPrivilege Otherwise 0	1 if there is SeTcbPrivilege Otherwise 0

Mask of Processes				
Bit 1	Bit 2	Bit 3	Bit 4	Bit 5
Always 1	Always 1	0 if there is "ccSvcHst.exe" or "NS.exe" Otherwise 1	0 if "avp.exe" is found, Otherwise 1	Always 1

Activities	Required Bits	
	Mask of Privileges	Mask of Processes
Record MBR with a ransom requirement	Bit 2 is set	Bit 4 is set
Zeroing in the MBR	Bit 2 is set	Reset bit 4
Running mimikatz	Bit 2 is set	Bit 1 is set
PsExec entry in dllhost.dat	If bit 2 or 3 is set - entry in C: \ Windows	Bit 2 is set
Encrypt files on local disks before rebooting	In application data in another case	Bit 5 is set
Using exploits for SMBs	-	Bit 3 is set
Reboot the OS by calling NtRaiseHardError or InitiateSystemShutdownExW or ExitWindowsEx	-	Bit 4 is set

This report is a property of ISSP – Information Systems Security Partners and shall not be duplicated, distributed or otherwise disseminated as a whole report without prior written consent from ISSP. Reference to ISSP – Information Systems Security Partners is mandatory in case of quoting each and any part of this report.