Research
Vulnerability Research
Malware Research

Trojan-Downloader.Win32.Sofacy.B

TSL ID	TSL20150713-04
Severity	Moderate
Description	Trojan-Downloader.Win32.Sofacy.B is a Trickler that targets the Windows platform. It is reported that this malware has been used in targeted attacks against corporations operating in the military, diplomatics, nuclear, telecommunications, and defense industrial, among others. This malware reportedly spreads to other systems through exploitation of the Java vulnerability identified as CVE-2015-2590, the Flash vulnerability identified as CVE-2015-5119 and the Microsoft Office vulnerability identified as CVE-2015-2424 leveraged by Tsar Team also know as APT28, Operation Pawn Storm, Sednit group and Fancy Bear. This malware sends out system information and accepts commands from a control server. The supported commands would allow an attacker to download and execute files on the infected system.
Affected Products	• Microsoft Windows All Versions
File Hashes	MD5: • DCF6906A9A0C970BCD93F451B9B7932A SHA1: • B8B3F53CA2CD64BD101CB59C6553F6289A72D9BB
Identifiers	Kaspersky: TROJAN.WIN32.AGENTB.BQAM Microsoft Malware Protection Center: TROJAN:WIN32/FOOSACE.J!DHA Symantec: TROJAN.SOFACY TrendMicro: TSPY_FAKEMS.C AVG: AGENT5.ACWW Avira: TR/AGENT.37888.359 Baidu: TROJAN.WIN32.AGENTB.BQAN BitDefender: TROJAN.GENERICKD.2562559 Cyren: W32/TROJAN.JZGN-4161 ESET: WIN32/AGENT.XIV Fortinet: W32/AGENT.XIA!TR iSightPartners: SOFACY NANO: TROJAN.WIN32.AGENTB.DUBJFP Tencent: WIN32.TROJAN.AGENTB.WWOC
References	http://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-update-trend-micro-discovers-new-java-zero-day-exploit/ http://www.isightpartners.com/2015/07/microsoft-office-zero-day-cve-2015-2424-leveraged-by-tsar-team/ http://www.welivesecurity.com/2015/07/10/sednit-apt-group-meets-hacking-team/
Related Threats	TSL20110908-01 - Trojan.Win32.Sofacy.A