Another Wiper Malware Discovered in Iran? « Hackmageddon.com

Yet another Sunday, yet another attack in Middle East.

57.7876 S2555	tigation have been done by Maher center i	targeted data wiping maheare	۰.
ID: SIGMENTS	121703		1116
Date: 2012-13	1-16		-
	increase. Here recombinations for collectional stands states testings affect	partitions and uses multip dispetation and	Oespite
recognized by		be walely distributed. This bargeted attack d attacks. The identified components of the	thest be to simple
recognized by design and it is	ext3-virus software. However, it is not considered to a not any sentently to the other sophisticated larget lowing table: HDS	be welely distributed. This targeted attack d attacks. The elevitified components of the Rame	thest be to simple
recognized by design and it is	ard-virus software. However, it is not considered to a not one sentiarity to the other sophisticidad torget lowing table: NOCS 13dd76677c16c25571f8c56a7f04e87h	Se woley distributed. This targeted attack d attacks. The identified components of the Bares GrooveMoniter.ave [dropper]	thest be to simple
recognized by design and it is	ard-virus software. However, it is not considered to soft any sentently to the other sophaticated target being tables 13617067703628571fftc96c370648776 fs/b000607167263521fftc96c370648776 fs/b000607167263521fftc96c370648776	Se volkly distributed. This targeted attack d attacks. The starsfield components of the Rame GraveMonitor.com [dropper] jubcet.com	thest be to simple
recognized by design and it is	ard-virus software. However, it is not considered to a not one sentiarity to the other sophisticidad torget lowing table: NOCS 13dd76677c16c25571f8c56a7f04e87h	Se woley distributed. This targeted attack d attacks. The identified components of the Bares GrooveMoniter.ave [dropper]	thest be to simple
recognized by design and it is	ard-virus software. However, it is not considered to soft any sentently to the other sophaticated target being tables 13617067703628571fftc96c370648776 fs/b000607167263521fftc96c370648776 fs/b000607167263521fftc96c370648776	Se volkly distributed. This targeted attack d attacks. The starsfield components of the Rame GraveMonitor.com [dropper] jubcet.com	thead be to simple

Maher Center, the <u>Iranian Computer Emergency</u> <u>Response Team / Coordination Center</u> has just released a scant <u>report</u> concerning another (alleged) cyber attack targeting Iran.

Few information is available so far regarding this new targeted attack. The malware, simple in design and hence apparently unrelated to the other sophisticated cyber attacks targeting the same area, seems to have an efficient design and wiping features. According to the statement, the malware "wipes files on different drives in various predefined times. Despite its simplicity in design, the malware is efficient and can wipe disk partitions and user profile directories without being recognized by anti-virus software". However, it is not considered to be widely distributed. The report also publishes the MD5s of the five identitified components. Wiper malware samples are becoming increasingly common in Middle East. Of course the most known example so far is the massive cyber attack targeting <u>Saudi Aramco</u>, occurred in August 2012 and targeting 30,000 internal workstations. Few days ago, the <u>final results</u> of the investigations were unveiled, suggesting that the attack was carried on by organized foreign hackers, and aimed "*to stop pumping oil and gas to domestic and international markets*" with huge impacts on the national economy of the kingdom.

The next hours will tell us if we are in front of a similar scenario, or the statement is rather an attempt of propaganda aimed to emphasize Iranian defensive capabilities.

Like this:

Be the first to like this.