‘WIPER’ ATTACKS:
How Sony Hack Compares

A Nov. 24 cyber-attack against Sony Pictures Entertainment represents the first time that a destructive "wiper" malware attack has been launched against a business operating in the United States, security experts say.

Wiper malware is dangerous, because it can erase data from PC and file-server hard drives and delete the master boot record, so the machines can no longer boot.

Kaspersky Lab reports that the “Destover” attack against Sony shares "extraordinary" similarities with two earlier wiper attacks: "Shamoon," which infected Saudi Aramco; and "Dark Seoul" malware, which infected South Korean banks and broadcasters.

Description:
Movie and television studio
When: Nov. 24, 2014
Malware labeled: Destover/Wipall
Systems wiped: Unknown
Credit claimed by: Guardians of Peace

Description:
South Korean banks/insurers Jeju, NongHyup and Shinhan; broadcasters KBS, MBC and YTN
When: March 20, 2013
Malware labeled: Dark Seoul
Systems wiped: 32,000 (estimated)
Credit claimed by: Whois, as well as New Romantic Cyber Army Team

Description:
Saudi Arabia's state-owned - and the world's largest - oil, gas and petroleum producer
When: Aug. 15, 2012
Malware labeled: Shamoon
Systems wiped: 30,000 (estimated)
Credit claimed by: Cutting Sword of Justice

Significant Similarities

Characteristics	Description	Destover Sony	Dark Seoul South Korea	Shamoon Saudi Aramco
Political motivation	Security experts say the attack has an obvious political impetus		✓	✓
EldoS RawDisk	Malware used commercially available software to directly access Windows drives	✓	✓	✓
Master Boot Record deleted	Deleting MBR prevents system from booting	✓	✓	✓
Unix/Linux scripts	Malware uses scripts to erase Linux partitions		✓	
Data wiped	Data deleted from PC and file-server hard drives	✓	✓	✓
Data leaked	Sensitive internal information and/or PII leaked	✓		✓
Aesthetics	Similar warning images displayed on hacked PCs (fonts, wording, graphics)	✓	✓	✓
Malware compiled	Time between when malware was compiled and malware was “detonated”	< 2 days	< 2 days	< 5 days
Positive ID	The true identity of the attackers	?	?	?

Sources: Kaspersky Lab, McAfee, EdgeWave

To learn more about data breach response, prevention and detection, visit www.databreachtoday.com.

Data Breach TODAY
Prevention. Response. Notification.