Скрипт имеет двойную обфускацию, в 1.txt представлен первая ступень обфускация, дешифрация хеша:

I58mjY6n3('98B6a29aa5aeB4a152B07869A7908b9d68725C8B9b7Aac749….’);

После дешифрации полученный код выполняется в eval:

eval(M6Nnm6jY0);

Данный код из eval выше представлен в файле 2.txt

Там такая же структура и аналогия но имена переменных изменены, после второй дешифрации кода полученый результат так же выполняется через eval:

eval(ud7a00v7W);

Сам код и его выполнение представлен в файле 3.txt

Код представляет собой атаку на компонент ActiveX с переполнением буфера

В условии вызываются функции осуществляющие перебор уязвимостей и выполнение произвольного кода на машине жертвы. Одна функция = одна уязвимость:

if (n0lterOf() || DnCWiFOj() || SOhxTHtY() || u5r\_Qafm() || Fv2QJVho() || uzbeukYW() || bF4sn2HS()) { }

Если атака удачна то на машине жертвы запускается участок кода осуществляющий какие либо действия, установку инсталла зачастую.

var name = "c:\\win"+ozavD28v(4)+".exe";

Часть уязвимостей представленых в коде:

<http://www.securitylab.ru/vulnerability/306361.php>

<https://tools.cisco.com/security/center/viewAlert.x?alertId=14972>

<http://www.securitylab.ru/vulnerability/274641.php>

<http://www.securityfocus.com/bid/23224>

<https://www.cisecurity.org/advisory/multiple-vulnerabilities-in-apple-quicktime-could-allow-remote-code-execution/>