Bundesamt für Verfassungsschutz

Köln, 18. Juni 2020

BfV Cyber-Brief

Nr. 01/2020

- Hinweis auf aktuelle Angriffskampagne -

Kontakt:
Bundesamt für Verfassungsschutz
Cyberabwehr
☎ 0221/792-2600

Bedrohung deutscher Stellen durch Cyberangriffe der Gruppierung Ke3chang

Aktuelle Hinweise deuten auf aktuelle Cyberangriffs-Aktivitäten der Gruppierung Ke3Chang gegen Wirtschaftsunternehmen und politische Einrichtungen hin.

Sachverhalt

Ke3chang[1] ist eine mutmaßlich seit 2010 aktive Cyberspionagegruppierung, die bereits in der Vergangenheit durch Angriffe auf Regierungseinrichtungen, diplomatische Ziele und Wirtschaftsunternehmen auf sich aufmerksam machte. Mitte 2019 warnte z.B. der IT-Sicherheitsdienstleister ESET vor Aktivitäten von Ke3chang.[2]

Nach Erkenntnissen der Cyberabwehr des Bundesamtes für Verfassungsschutz sind diese Angriffe Teil einer seit mehreren Jahren andauernden, umfangreichen Cyberspionagekampagne in verschiedenen Teilen Europas. Zum Schutz deutscher Stellen werden mit diesem Cyberbrief Detektionsregeln und technische Indikatoren (Indicators of Compromise) zur Verfügung gestellt, durch die Unternehmen und öffentliche Einrichtungen Infektionen mit aktuellen Versionen der durch Ke3chang verwendeten Schadsoftware namens Ketrican feststellen können.[3]

Vorgehensweise von Ke3chang

Folgende Verhaltensweisen zeichnen den Akteur im Rahmen dieser Cyberspionagekampagne aus:

- Nutzung des HTTP-Protokolls zur Kommunikation
- Einheitliche Muster in den Kommunikationsabständen (feste Zeitintervalle zwischen dem Beaconing)
- Schwächung des Internet Explorers durch Anpassung der entsprechenden Registry-Einträge
- Intensive Nutzung von cmd.exe zur Ausführung von Befehlen
- Geringe Anzahl infizierter Maschinen
- Nutzung von Standard- bzw. OpenSource-Tools wie z. B. RAR-Datenkompression oder Mimikatz

Bei der Nutzung der Schadsoftware Ketrican:

- Befehle werden zwischen Schlüsselwörtern in aufgerufenen Webseiten an den kompromittierten Client ausgeliefert: *good<Befehl>bad, white<Befehl>purple oder nice<Befehl>say*. Derzeit ist für diese Schlüsselwörter noch keine eindeutige Systematik erkennbar. Die Befehle sind verschlüsselt (AES128 oder XOR).
- Die technische Analyse von Ketrican-Samples hat ergeben, dass die Schadsoftware selbst keine Persistenz im System herstellt. Es wird daher eher davon ausgegangen, dass ein anderer Mechanismus (z. B. ein Dropper) eine Persistenz der Ketrican-Backdoor einrichtet.

1 Ke3chang wird durch IT-Sicherheitsunternehmen auch unter den Bezeichnungen APT15, APT25, Vixen Panda und Metushy geführt.

2 Vgl. “Okrum and Ketrican: An overview of recent Ke3chang group activity” vom 18.07.19, in www.welivesecurity.com

3 Die Cyberabwehr des Bundesamtes für Verfassungsschutz bedankt sich bei der Deutschen Cyber-Sicherheitsorganisation GmbH (DCSO) für die Prüfung der Detektionsregeln.

Technische Analyse

Die folgenden Informationen basieren auf der Analyse zahlreicher Ketrican-Samples durch die Cyberabwehr des Bundesamtes für Verfassungsschutz.

Abbildung 1 zeigt den typischen Ablauf einer Ketrican-Instanz, der sich aus einer Initialisierungs- und Operationsphase zusammensetzt. Im Folgenden werden deren Funktionsweisen näher erläutert.

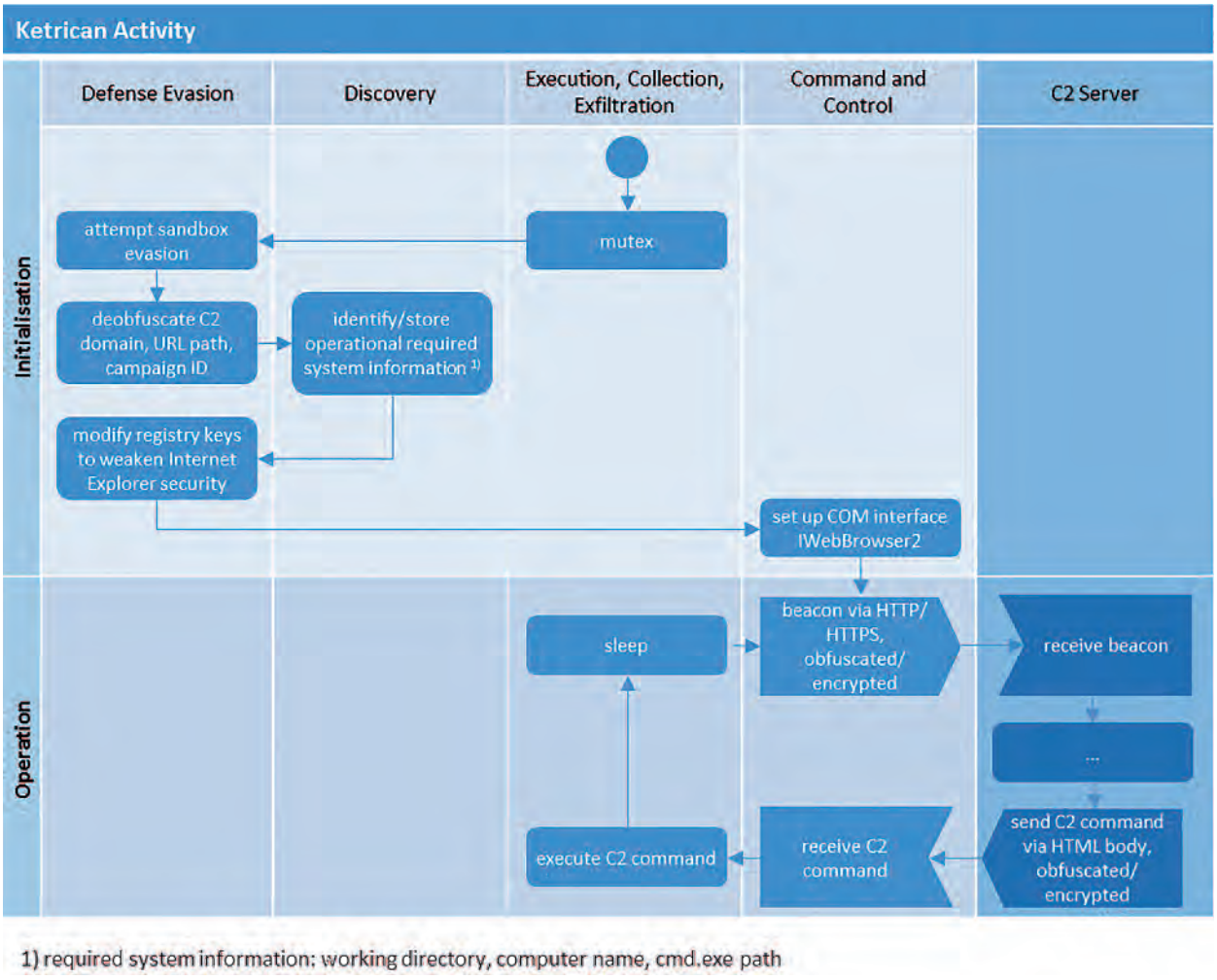

Abbildung 1: Typischer Ablauf einer-Ketrican Instanz nach Start bis hin zum angreifergesteuerten Betrieb der Schadsoftware.

Initialisierungsphase (siehe Abb. 2):

1 Nach dem Start verhindert Ketrican mittels eines Mutex[4] das Ausführen einer weiteren Instanz der Schadsoftware.

2 Im Rahmen der "Defense Evasion" versucht Ketrican durch eine lange Inaktivitätszeit in der Initialisierungsphase (API-Funktion *Sleep*) bei Ausführung innerhalb von Sandbox-Umgebungen unentdeckt zu bleiben. Einige Varianten von Ketrican nutzen zusätzlich/alternativ die API-Funktion *GetTickCount*() in Verbindung mit einer rechenintensiven Befehlsschleife, um typische Sandbox-Mechanismen zu detektieren und die Schadsoftware ggf. ohne weitere Aktivität zu beenden.

4 Mutex (Abk. für englisch mutual exclusion) bezeichnet ein Verfahren zum wechselseitigen Ausschluss mehrerer Prozesse, die auf dieselbe Ressource zugreifen.

3 Im nächsten Schritt werden die in der Schadsoftware Base64-kodierte und verschlüsselte C2-Domain sowie URL-Pfade und eine Kampagnen-ID für die spätere Verwendung entschlüsselt. Dabei wird oft eine triviale XOR-Verschlüsselung verwendet.

4 Anschließend werden das *%temp%*-Verzeichnis, der Computername und der Pfad zur Betriebssystem-Shell (cmd.exe) bestimmt und für die weitere Verwendung in globalen Variablen gespeichert. Im *%temp%*-Verzeichnis werden im Verlauf der Schadsoftwareausführung alle erzeugten/heruntergeladenen Dateien abgelegt. Der Computername wird verwendet, um daraus eine spezifische Opfer-ID zu erzeugen, die in der Kommunikation der Schadsoftware mit dem C2-Server zur Identifikation dient.

5 Da die Schadsoftware die Engine des Internet Explorers für die C2-Kommunikation über HTTP/HTTPS verwendet, werden vor der ersten Kommunikationsaufnahme diverse Sicherheitseinstellungen des Internet Explorers in der Windows-Registry geändert (siehe **Anhang – Registry Keys**). Zur Änderung der Registry kommt z. B. die PowerShell zum Einsatz.

6 Anschließend wird eine Referenz auf das COM-Interface IWebBrowser2 angelegt, um die C2-Kommunikation über die Engine des Internet Explorers zu ermöglichen. Hiermit ist die Initialisierungsphase der Schadsoftware abgeschlossen.

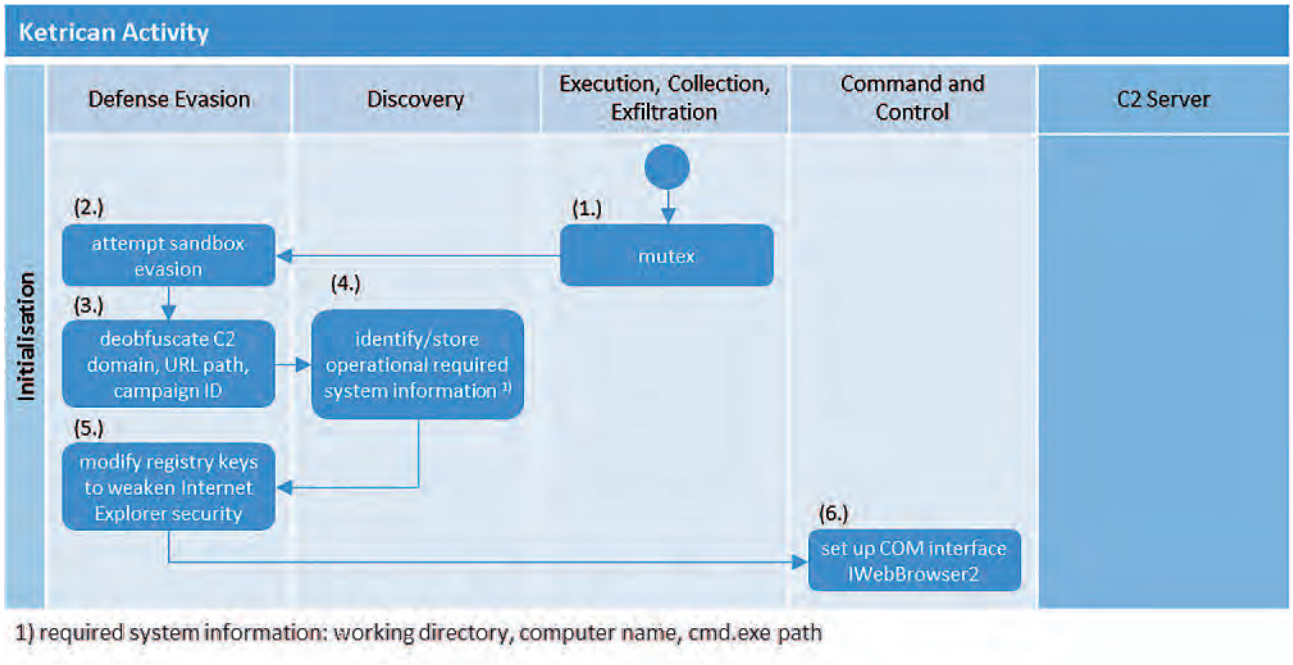

Abbildung 2: Ablauf der Initialisierungsphase von Ketrican

Operationsphase (siehe Abb. 3):

In regelmäßigen Abständen sendet die Schadsoftware HTTP/HTTPS-Anfragen an den C2-Server (Beacon) (I.) und erwartet als Antwort (II.) die Übermittlung einer HTML-Seite mit speziellen Schlüsselwörtern, z. B. "*nice*" und "*say*", zwischen denen sich die Steuerkommandos in Base64-kodierter und verschlüsselter Form befinden.

Die HTTP/HTTPS-Anfragen enthalten als Parameter in verschlüsselter Form den Computernamen, die zuvor bestimmte Opfer-ID sowie die im Sample enthaltene Kampagnen-ID. Als Verschlüsselung kommen AES (im Betriebsmodus CBC) oder XOR zum Einsatz, wobei die notwendigen Schlüssel

gleichzeitig übermittelt werden. So wird z. B. bei Verwendung von AES der Schlüssel in den ersten 16 Byte und der Initialisierungsvektor in den letzten 16 Byte der Payload übermittelt. Die Kombination aus AES-Schlüssel, verschlüsselten Daten und Initialisierungsvektor ist zudem Base64-kodiert.

Das Steuerkommando des C2-Servers ist auf gleiche Weise verschlüsselt (inkl. zufällig generiertem Schlüssel/Initialisierungsvektor) wie die Anfrage.

Die aufgerufene URL variiert je Anfrage nach einem vorgegebenen Muster in der Pfad-Komponente. Ein Merkmal scheint der Aufruf von aspx-Dateien zu sein.

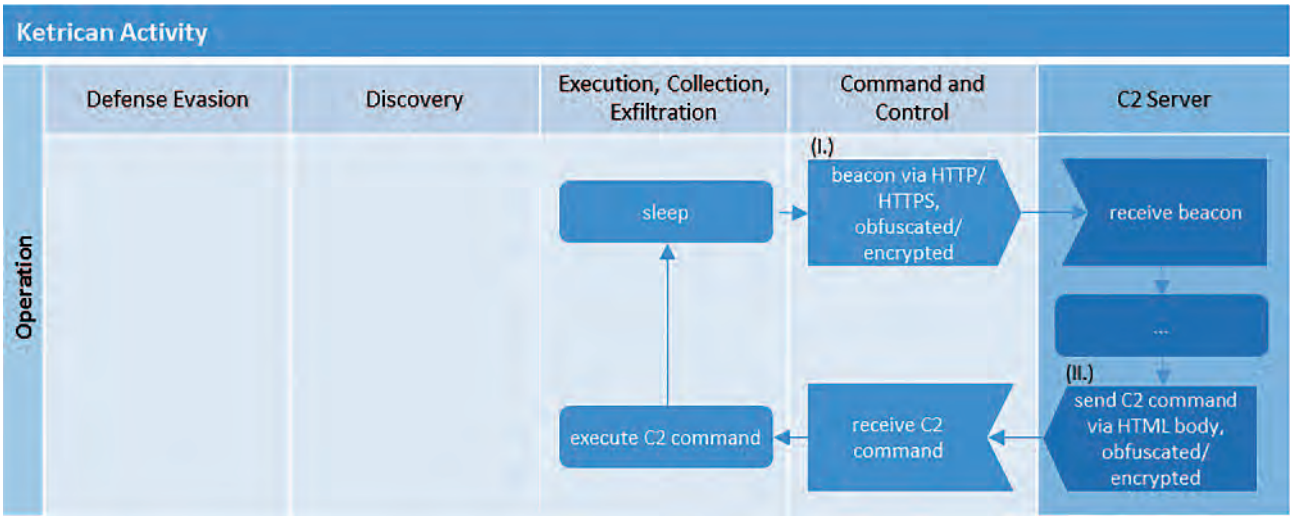

Abbildung 3: Operationsphase bzw. Angreifer-gesteuerter Betrieb von Ketrican

Ketrican erlaubt über die Steuerkommandos:

- die Ausführung beliebiger übermittelter Kommandos und Dateien mittels cmd.exe
- die Ausführung von Dateien mittels API Funktion *CreateProcessW()*
- das Einlesen lokaler Dateien und Übermittelung des Inhalts an den C2-Server
- den Download von Dateien vom C2-Server
- Änderungen des Beacon-Intervalls

Ergebnisse von ausgeführten Kommandos oder Dateien werden im *%temp%*-Verzeichnis in einer Logdatei gespeichert, die nach der Übertragung an den C2-Server vom infizierten System gelöscht wird. Übermittlungen an den C2-Server erfolgen dabei stets verschlüsselt nach obigem Schema. Hierbei wird je Übermittlung ein neuer Schlüssel/Initialisierungsvektor verwendet. Wie bei dem Beacon wird ebenfalls die Pfad-Komponente der URL nach einem vorgegebenen Muster variiert. Auch hier scheint der Aufruf von aspx-Dateien ein besonderes Merkmal darzustellen.

Mögliche Erhöhung der Sichtbarkeit einer Infektion

Die eingesetzte Schadsoftware – neben einigen Mechanismen zur Erschwerung der Analyse – wird individuell angepasst. Die durch die Cyberabwehr des Bundesamtes für Verfassungsschutz mit diesem Cyber-Brief bereitgestellte Detektionsregel ermöglicht jedoch eine Erkennung zahlreicher Varianten der Ketrican-Schadsoftwarefamilie. Zudem bietet es sich an, möglicherweise betroffene Systeme auf das Vorhandensein der spezifischen Registry-Einträge zu überprüfen (**siehe Anhang – Registry Keys**). Diese Registry-Einträge sind zwar als solche legitim, das Auftreten mehrerer der genannten Keys in Kombination spricht jedoch mit hoher Wahrscheinlichkeit für eine Infektion mit Ketrican.

Handlungsempfehlung

Die Cyberabwehr des Bundesamtes für Verfassungsschutz empfiehlt die Überprüfung der eigenen Netzwerk-Hosts mit der nachfolgenden Detektionsregel.

Darüber hinaus bieten wir Ihnen zusätzliche Hintergrundinformationen an. Hierzu stehen wir Ihnen unter folgenden Kontaktdaten gerne zur Verfügung:

Tel.: 0221-792-2600 oder

E-Mail: poststelle@bfv.bund.de

Cyberabwehr BfV

Abbildung nach MITRE ATT&CK[5] Schema

ID	Tactic	Name
T1005	Collection	Data from Local System
loioiuKetrican allows to collect the output from the command-line interface as well as the content of files.		
T1001	Command and Control	Data Obfuscation
Ketrican obfuscates C2 traffic using Base64 encoding and receives C2 commands hidden in a HTML body.		
T1024	Command and Control	Custom Cryptographic Protocol
Ketrican variants encrypt C2 traffic using a XOR cipher.		
T1032	Command and Control	Standard Cryptographic Protocol
Ketrican variants encrypt C2 traffic using AES (in CBC mode).		
T1043	Command and Control	Commonly Used Port
Ketrican uses TCP port 80 or 443 for C2 communication.		
T1071	Command and Control	Standard Application Layer Protocol
Ketrican uses HTTP or HTTPS to contact the C2 server through the Internet Explorer Engine using the IWebBrowser2 COM interface.		
T1105	Command and Control	Remote File Copy
Ketrican allows to upload or download files from the C2 server.		
T1132	Command and Control	Data Encoding
Ketrican encodes C2 traffic with Base64.		
T1027	Defense Evasion	Obfuscated Files or Information
Ketrican uses Base64 and XOR cipher to obfuscate strings.		
T1066	Defense Evasion	Indicator Removal from Tools
Ketrican samples appear to be compiled and modified for each individual victim. Furthermore, Ketrican receives regular updates to evade anti-virus detection.		
T1089	Defense Evasion	Disabling Security Tools
Ketrican weakens Internet Explorer security settings by changing Registry keys.		
T1107	Defense Evasion	File Deletion
Ketrican deletes files (containing previously collected data) after upload to the C2 server.		
T1112	Defense Evasion	Modify Registry
Ketrican modifies several Registry keys related to Internet Explorer security.		
T1140	Defense Evasion	Deobfuscate/Decode Files or Information
Ketrican uses Base64 and XOR cipher to deobfuscate strings.		

5 URL: https://attack.mitre.org

ID	Tactic	Name
T1497	Defense Evasion, Discovery	Virtualization/Sandbox Evasion
Ketrican uses a combination of delayed activity after start and the API function GetTickCount to evade/detect a sandbox environment.		
T1082	Discovery	System Information Discovery
Ketrican collects the computer name and uses it to generate a victim ID.		
T1059	Execution	Command-Line Interface
Ketrican allows to run arbitrary commands on the command-line interface.		
T1086	Execution	PowerShell
Ketrican variants use PowerShell commands to modify Registry keys.		
T1106	Execution	Execution through API
Ketrican allows to run an application via API utilizing CreateProcessW.		
T1041	Exfiltration	Exfiltration Over Command and Control Channel
Ketrican exfiltrates data over the C2 channel.		

Detektionsregeln

Yara-Regel „Ketrican“ – zur Erkennung verschiedener Varianten der Schadsoftware „Ketrican“

```
rule ketrican
{
   strings:
      $r1=”WarnonZoneCrossing” wide ascii
      $r2=”WarnOnPostRedirect” wide ascii
      $r3=”ShownVerifyBalloon” wide ascii
      $r4=”DisableFirstRunCustomize” wide ascii
      $r5=”Internet Connection Wizard” wide ascii

      $f21={57 61 72 6e}
      $f22={72 6e 6f 6e}
      $f23={5a 6f 6e 65}
      $f24={43 72 6f 73}
      $f25={73 69 6e 67}

      $f31={72 6E 4F 6E}
      $f32={50 6F 73 74}
      $f33={52 65 64 69}
      $f34={72 65 63 74}

      $f51={53 68 6f 77}
      $f52={6f 77 6e 56}
      $f53={65 72 69 66}
      $f54={79 42 61 6c}
      $f55={6c 6f 6f 6e}

      $f61={44 69 73 61}
      $f62={62 6c 65 46}
      $f63={69 72 73 74}
      $f64={52 75 6e 43}
      $f65={75 73 74 6f}
      $f66={6d 69 7a 65}

      $f71={49 6e 74 65}
      $f72={74 65 72 6e}
      $f73={65 74 20 43}
      $f74={6f 6e 6e 65}
      $f75={63 74 69 6f}
      $f76={6e 20 57 69}
      $f77={7a 61 72 64}

      $clsid1 = “0002DF01-0000-0000-C000-000000000046” wide ascii
      $clsid2 = {01 DF 02 00 00 00 00 00 C0 00 00 00 00 00 00 46}
      $iid1 = {61 16 0C D3 AF CD D0 11 8A 3E 00 C0 4F C9 E2 6E}
      $iid2 = “D30C1661-CDAF-11D0-8A3E-00C04FC9E26E” wide ascii
```

```
      $s1 = “CoInitialize” wide ascii

   condition:
      uint16(0) == 0x5A4D and
      filesize < 1000KB and
      $s1 and
      (
        (4 of ($f2*) and 4 of ($f3*) and 4 of ($f5*) and 5 of ($f6*) and 5 of ($f7*)) or
        4 of ($r*)
      ) and
      (1 of ($clsid*)) and
      (1 of ($iid*))
}
```

Registry Keys

HKCU\Software\Microsoft\Internet Connection Wizard\Completed = 1

HKCU\Software\Microsoft\Internet Explorer\Main\Check_Associations = ‘no’

HKCU\Software\Microsoft\Internet Explorer\Main\DEPOff = 1

HKCU\Software\Microsoft\Internet Explorer\Main\DisableFirstRunCustomize = 2

HKCU\Software\Microsoft\Internet Explorer\PhishingFilter\Enabled = 1

HKCU\Software\Microsoft\Internet Explorer\PhishingFilter\ShownVerifyBalloon = 3

HKCU\Software\Microsoft\Internet Explorer\Recovery\AutoRecover = 2

HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\IEHardenIENoWarn = 0

HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\WarnOnPostRedirect = 0

HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\WarnonBadCertRecving = 0

HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\WarnonZoneCrossing = 0

HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\ZoneMap\IEHarden = 0

HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3\2500 = 3