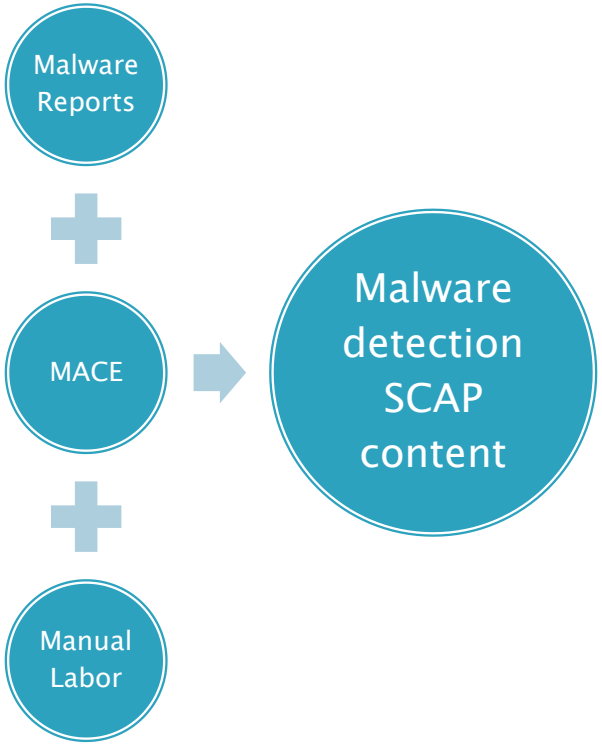
Automated Creation of SCAP Content

Automated Malware Analysis

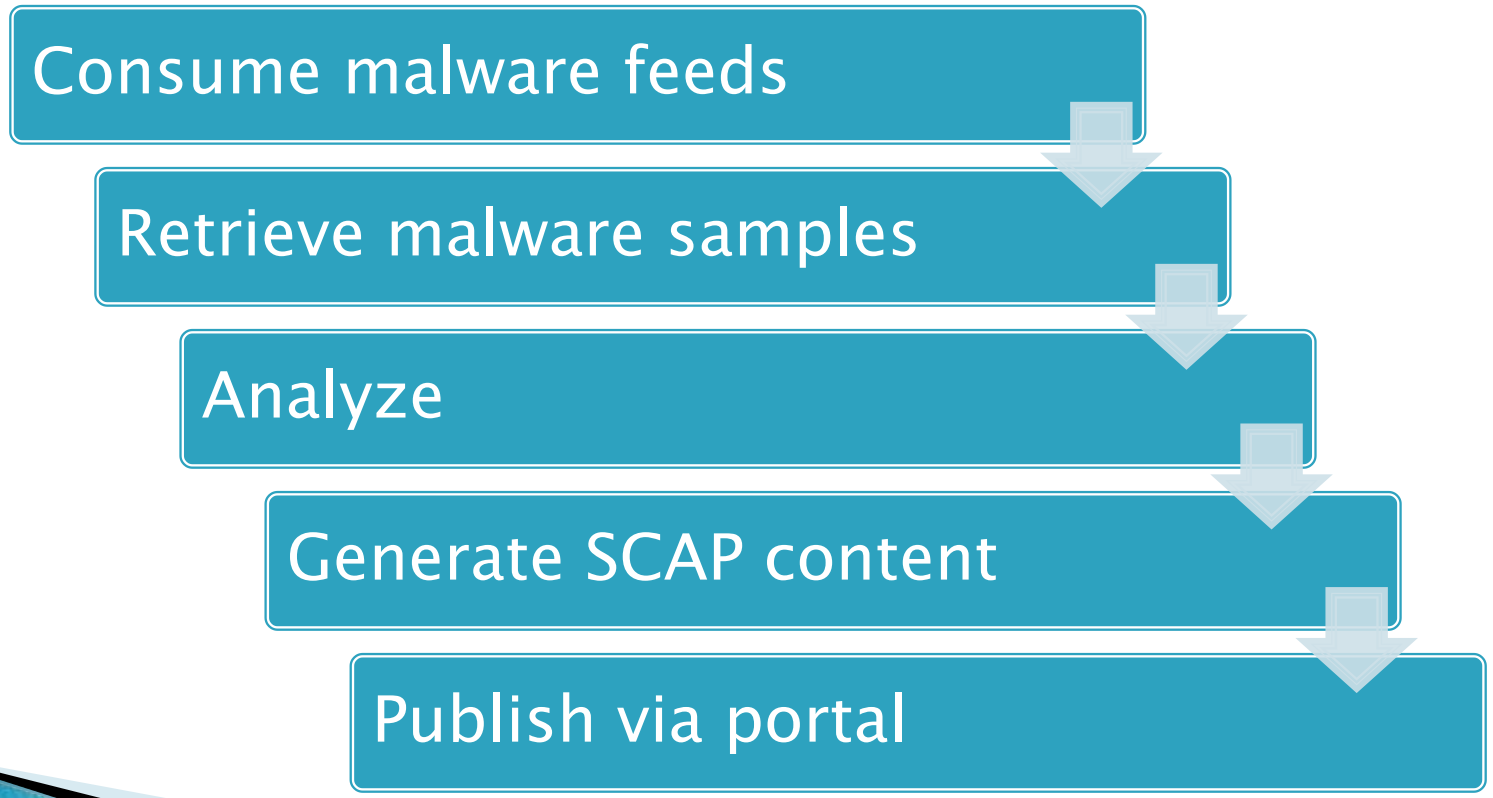
The past – one year ago

- MACE – Malware Content Editor
  - Manual creation of SCAP content for detection of malware



The present

- AMA – Automated Malware Analysis



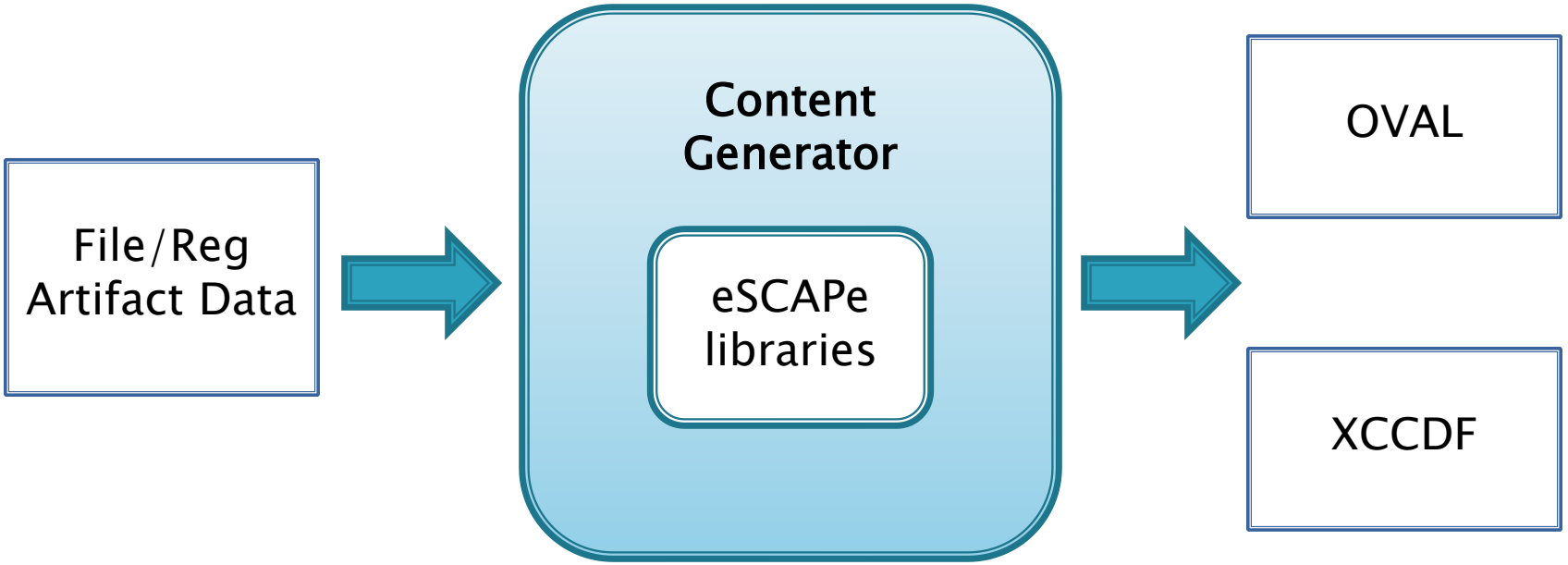
Malware Downloader

- Consumes multiple feeds of public malware information
- Downloads new malware daily
  - Over 20GB of malware downloaded so far
  - Hundreds of types of malware
    - Botnet binaries
    - Exploit kits
    - Malicious PDF files
    - Fake AV binaries
    - Ransomware
    - And on and on…

Analysis

- Proprietary process to analyze downloaded malware
- Produces a variety of useful data
  - Some attribution information
  - Disassembly output
  - Full HTTP download headers
  - Packer identification
  - File system and registry artifacts

Generate SCAP content



eSCAPe

- Enhanced SCAP Editor
- Released under GPLv3
  - http://www.g2-inc.com/escape

- Cross platform Java application
  - Content editing tool
  - Libraries
    - AMA calls libraries using Jython

SCAP Output

- OVAL
  - 1 Definition
    - Class = vulnerability
    - Multiple criterion
  - 1 Test per artifact
  - Objects, States, Variables as needed
- XCCDF
  - One rule
- CPE Dictionary / CPE OVAL not included

Example: Zeus

- Keystroke logging trojan geared towards the compromise of various credentials and sensitive data:
  - Online banking information
  - Social networking sites
  - Email accounts
- Web form field insertion
- Used in several large worldwide botnets ("Kneber" was a recent example)

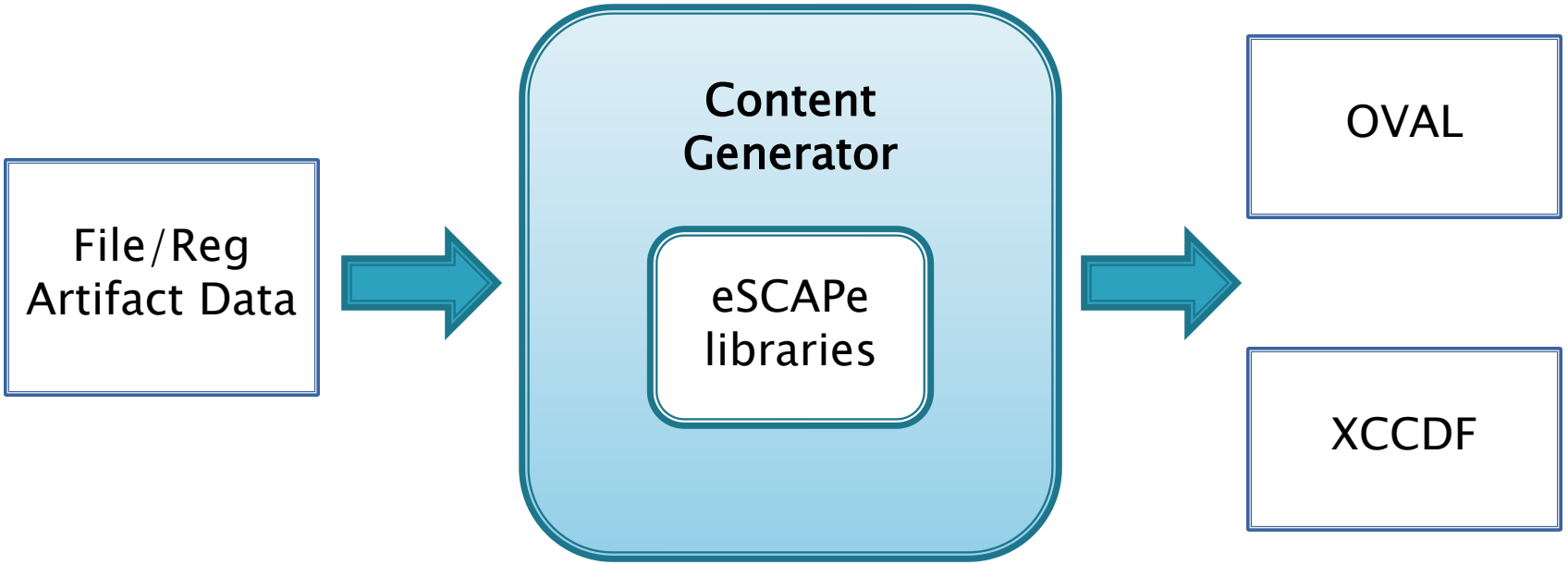
Zeus artifacts – files

- %System%\sdra64.exe
  - MD5: b098bb0468bbf4f356bdf86207eed751
- %System%\lowsec\local.ds
  - MD5: d41d8cd98f00b204e9800998ecf8427e
- %System%\lowsec\user.ds
  - MD5: d41d8cd98f00b204e9800998ecf8427e
- %System%\lowsec\user.ds.lll
  - MD5: da09db1b5115640439 0d4b20c6266a2c

Zeus artifacts – registry

- Key: HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\{43BF8CD1-C5D5-2230-7BB2-98F22C2B7DC6}
- Value: {3039636B-5F3D-6C64-6675-69687066726 5} = F7 09 F2 0D
- And others…

Generate SCAP content



Zeus OVAL: Definitions

```
<?xml version="1.0" encoding="UTF-8"?>
<oval_definitions xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:oval="http://oval.mitre.org/XMLSchema/oval-common-5"
  xmlns:oval-def="http://oval.mitre.org/XMLSchema/oval-definitions-5"
  xmlns:independent-def="http://oval.mitre.org/XMLSchema/oval-definitions-5#independent"
  xmlns:windows-def="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows"
  xsi:schemaLocation="http://oval.mitre.org/XMLSchema/oval-definitions-5 oval-definitions-schema.xsd http://oval.mitre.org/XMLSchema/oval-definitions-5#windows
windows-definitions-schema.xsd http://oval.mitre.org/XMLSchema/oval-definitions-5#independent independent-definitions-schema.xsd
http://oval.mitre.org/XMLSchema/oval-common-5 oval-common-schema.xsd">
  <generator>
    <oval:product_name>AMA</oval:product_name>
    <oval:schema_version>5.3</oval:schema_version>
    <oval:timestamp>2010-09-22T04:42:18.876-05:00</oval:timestamp>
  </generator>
  <definitions>
    <definition id="oval:g2.com:def:1" version="1" class="vulnerability">
      <metadata>
        <title>Zeus Botnet</title>
        <affected family="windows">
          <platform>Microsoft Windows 2000</platform>
          <platform>Microsoft Windows XP</platform>
          <platform>Microsoft Windows Vista</platform>
          <platform>Microsoft Windows 7</platform>
          <platform>Microsoft Windows Server 2003</platform>
          <platform>Microsoft Windows Server 2008</platform>
        </affected>
        <description>Zeus botnet infection is present on the system.</description>
      </metadata>
      <criteria operator="OR">
        <criterion test_ref="oval:g2.com:tst:1" comment="Filehash Test for 'sdra64.exe'"/>
        <criterion test_ref="oval:g2.com:tst:2" comment="Filehash Test for 'local.ds'"/>
        <criterion test_ref="oval:g2.com:tst:3" comment="Filehash Test for 'user.ds'"/>
        <criterion test_ref="oval:g2.com:tst:4" comment="Filehash Test for 'user.ds.lll'"/>
        <criterion test_ref="oval:g2.com:tst:5" comment="Registry Test for 'HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Network\UID'"/>
        <criterion test_ref="oval:g2.com:tst:6" comment="Registry Test for 'HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\{43BF8CD1-C5D5-
2230-7BB2-98F22C2B7DC6}\{3039636B-5F3D-6C64-6675-696870667265}'"/>
        <criterion test_ref="oval:g2.com:tst:7" comment="Registry Test for 'HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\{43BF8CD1-C5D5-
2230-7BB2-98F22C2B7DC6}\{33373039-3132-3864-6B30-303233343434}'"/>
      </criteria>
    </definition>
  </definitions>
```

Zeus OVAL: Tests

```
<tests>
  <filehash_test xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#independent" id="oval:g2.com:tst:1" version="1" check="at least one"
check_existence="at_least_one_exists" comment="Filehash test for 'sdra64.exe'">
    <object object_ref="oval:g2.com:obj:1"/>
    <state state_ref="oval:g2.com:ste:1"/>
  </filehash_test>
  <filehash_test xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#independent" id="oval:g2.com:tst:2" version="1" check="at least one"
check_existence="at_least_one_exists" comment="Filehash test for 'local.ds'">
    <object object_ref="oval:g2.com:obj:2"/>
    <state state_ref="oval:g2.com:ste:2"/>
  </filehash_test>
  <filehash_test xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#independent" id="oval:g2.com:tst:3" version="1" check="at least one"
check_existence="at_least_one_exists" comment="Filehash test for 'user.ds'">
    <object object_ref="oval:g2.com:obj:3"/>
    <state state_ref="oval:g2.com:ste:3"/>
  </filehash_test>
  <filehash_test xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#independent" id="oval:g2.com:tst:4" version="1" check="at least one"
check_existence="at_least_one_exists" comment="Filehash test for 'user.ds.lll'">
    <object object_ref="oval:g2.com:obj:4"/>
    <state state_ref="oval:g2.com:ste:4"/>
  </filehash_test>
  <registry_test xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows" id="oval:g2.com:tst:5" version="1" check="at least one"
check_existence="at_least_one_exists" comment="Registry test for 'HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Network\UID'">
    <object object_ref="oval:g2.com:obj:5"/>
    <state state_ref="oval:g2.com:ste:5"/>
  </registry_test>
  <registry_test xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows" id="oval:g2.com:tst:6" version="1" check="at least one"
check_existence="at_least_one_exists" comment="Registry test for 'HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\{43BF8CD1-C5D5-2230-
7BB2-98F22C2B7DC6}\{3039636B-5F3D-6C64-6675-696870667265}'">
    <object object_ref="oval:g2.com:obj:6"/>
    <state state_ref="oval:g2.com:ste:6"/>
  </registry_test>
  <registry_test xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows" id="oval:g2.com:tst:7" version="1" check="at least one"
check_existence="at_least_one_exists" comment="Registry test for 'HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\{43BF8CD1-C5D5-2230-
7BB2-98F22C2B7DC6}\{33373039-3132-3864-6B30-303233343434}'">
    <object object_ref="oval:g2.com:obj:7"/>
    <state state_ref="oval:g2.com:ste:7"/>
  </registry_test>
</tests>
```

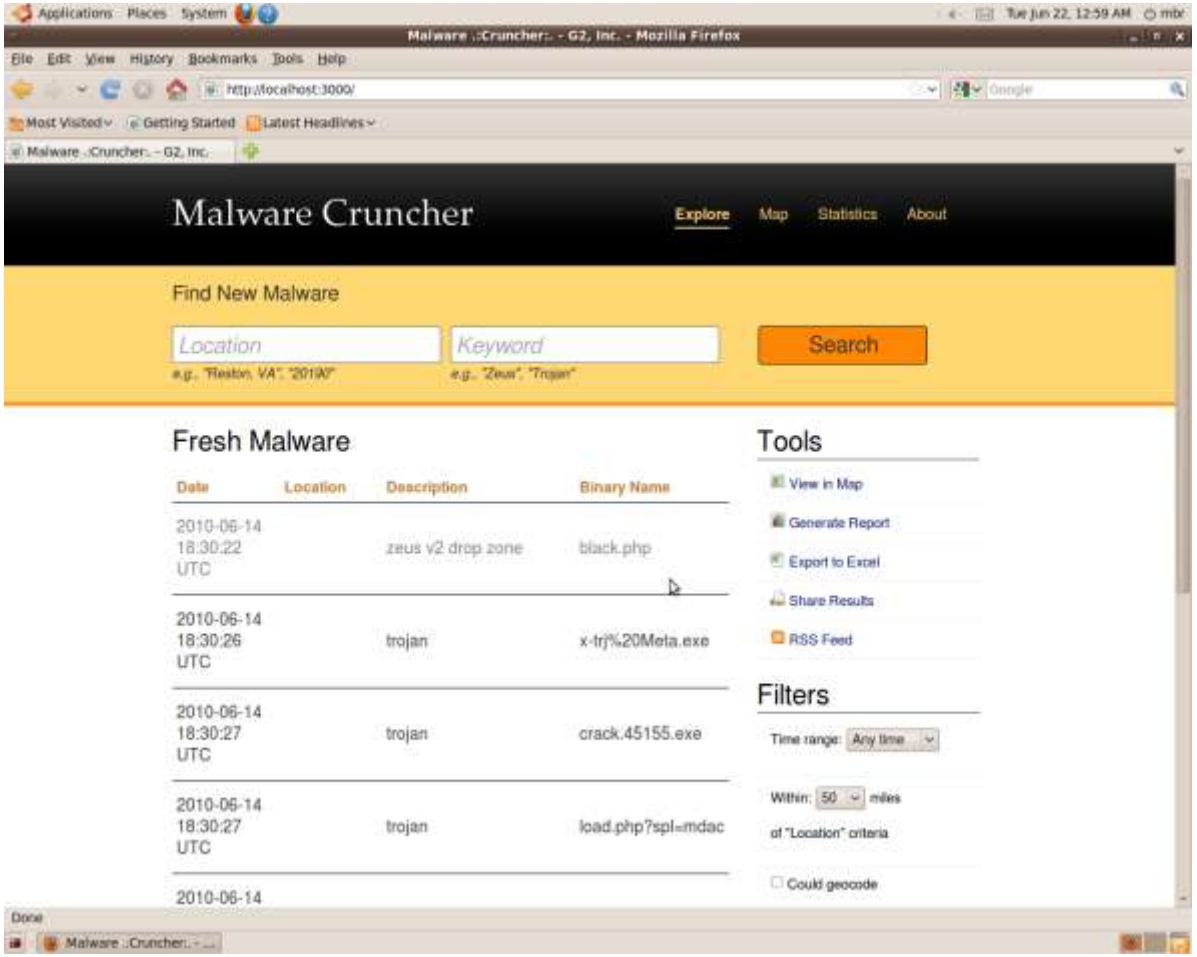
Zeus OVAL: Objects

```
<objects>
  <filehash_object xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#independent"
   id="oval:g2.com:obj:1" version="1" comment="Filehash object for 'sdra64.exe'">
   <behaviors recurse_direction="down" max_depth="-1"/>
   <path datatype="string" var_ref="oval:g2.com:var:2" var_check="all"/>
   <filename datatype="string">sdra64.exe</filename>
  </filehash_object>
  <filehash_object xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#independent"
   id="oval:g2.com:obj:2" version="1" comment="Filehash object for 'local.ds'">
   <behaviors recurse_direction="down" max_depth="-1"/>
   <path datatype="string" var_ref="oval:g2.com:var:1" var_check="all"/>
   <filename datatype="string">local.ds</filename>
  </filehash_object>
  <filehash_object xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#independent" id="oval:g2.com:obj:3" version="1" comment="Filehash object for 'user.ds'">
   <behaviors recurse_direction="down" max_depth="-1"/>
   <path datatype="string" var_ref="oval:g2.com:var:1" var_check="all"/>
   <filename datatype="string">user.ds</filename>
  </filehash_object>
  <filehash_object xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#independent" id="oval:g2.com:obj:4" version="1" comment="Filehash object for 'user.ds.lll'">
   <behaviors recurse_direction="down" max_depth="-1"/>
   <path datatype="string" var_ref="oval:g2.com:var:1" var_check="all"/>
   <filename datatype="string">user.ds.lll</filename>
  </filehash_object>
  <registry_object xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows" id="oval:g2.com:obj:5" version="1" comment="Registry object for
'HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Network\UID'">
   <hive datatype="string">HKEY_LOCAL_MACHINE</hive>
   <key datatype="string">SOFTWARE\Microsoft\Windows NT\CurrentVersion\Network</key>
   <name datatype="string">UID</name>
  </registry_object>
  <registry_object xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows" id="oval:g2.com:obj:6" version="1" comment="Registry object for
'HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\{43BF8CD1-C5D5-2230-7BB2-98F22C2B7DC6}\{3039636B-5F3D-6C64-6675-
696870667265}'">
   <hive datatype="string">HKEY_USERS</hive>
   <key datatype="string">.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\{43BF8CD1-C5D5-2230-7BB2-98F22C2B7DC6}</key>
   <name datatype="string">{3039636B-5F3D-6C64-6675-696870667265}</name>
  </registry_object>
  <registry_object xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows" id="oval:g2.com:obj:7" version="1" comment="Registry object for
'HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\{43BF8CD1-C5D5-2230-7BB2-98F22C2B7DC6}\{33373039-3132-3864-6B30-
303233343434}'">
   <hive datatype="string">HKEY_USERS</hive>
   <key datatype="string">.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\{43BF8CD1-C5D5-2230-7BB2-98F22C2B7DC6}</key>
   <name datatype="string">{33373039-3132-3864-6B30-303233343434}</name>
  </registry_object>
  <registry_object xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows" id="oval:g2.com:obj:9" version="1" comment="Registry object for '%systemroot%'">
   <hive datatype="string">HKEY_LOCAL_MACHINE</hive>
   <key datatype="string">SOFTWARE\Microsoft\Windows NT\CurrentVersion</key>
   <name datatype="string">SystemRoot</name>
  </registry_object>
</objects>
```

Zeus OVAL: States

```
 <states>
   <filehash_state xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#independent" id="oval:g2.com:ste:1" version="1" comment="Filehash state for 'sdra64.exe'">
     <md5 datatype="string" operation="equals" entity_check="all">b098bb0468bbf4f356bdf86207eed751</md5>
   </filehash_state>
   <filehash_state xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#independent" id="oval:g2.com:ste:2" version="1" comment="Filehash state for 'local.ds'">
     <md5 datatype="string" operation="equals" entity_check="all">d41d8cd98f00b204e9800998ecf8427e</md5>
   </filehash_state>
   <filehash_state xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#independent" id="oval:g2.com:ste:3" version="1" comment="Filehash state for 'user.ds'">
     <md5 datatype="string" operation="equals" entity_check="all">d41d8cd98f00b204e9800998ecf8427e</md5>
   </filehash_state>
   <filehash_state xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#independent" id="oval:g2.com:ste:4" version="1" comment="Filehash state for 'user.ds.lll'">
     <md5 datatype="string" operation="equals" entity_check="all">da09db1b51156404390d4b20c6266a2c</md5>
   </filehash_state>
   <registry_state xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows" id="oval:g2.com:ste:5" version="1" comment="Registry state for
'HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Network\UID'">
     <value datatype="string" operation="pattern match">^.*_00019B12$</value>
   </registry_state>
   <registry_state xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows" id="oval:g2.com:ste:6" version="1" comment="Registry state for
'HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\{43BF8CD1-C5D5-2230-7BB2-98F22C2B7DC6}\{3039636B-5F3D-6C64-6675-
696870667265}'">
     <value datatype="binary" operation="equals">f709f20d</value>
   </registry_state>
   <registry_state xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows" id="oval:g2.com:ste:7" version="1" comment="Registry state for
'HKEY_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Explorer\{43BF8CD1-C5D5-2230-7BB2-98F22C2B7DC6}\{33373039-3132-3864-6B30-
303233343434}'">
     <value datatype="binary" operation="equals">4709f20d</value>
   </registry_state>
 </states>
 <variables>
   <local_variable id="oval:g2.com:var:1" version="1" comment="Variable for '%systemroot%\lowsec" datatype="string">
     <concat>
       <object_component item_field="value" object_ref="oval:g2.com:obj:9"/>
       <literal_component>\system32\lowsec</literal_component>
     </concat>
   </local_variable>
   <local_variable id="oval:g2.com:var:2" version="1" comment="Variable for '%systemroot%'" datatype="string">
     <concat>
       <object_component item_field="value" object_ref="oval:g2.com:obj:9"/>
       <literal_component>\system32</literal_component>
     </concat>
   </local_variable>
 </variables>
</oval_definitions>
```

Malware Portal



Malware Portal – Details