Duping the machine: malware strategies, post Sandbox detection

VB2014

James Wyke

Senior Threat Researcher

SOPHOS

SOPHOS

Agenda

Agenda

- Introduction and background
- Example malware families
  - Andromeda
  - Simda
  - Vundo
  - Shylock
- Categorisation of techniques and goals
- Consequences of failure
- Protection
- Conclusion

SOPHOS

Introduction and Background

Introduction and Background

- Exponential growth in malware
- Too many samples for human analysts
- Solution – automated analysis
- Commercial and Open-Source products
- Majority VM based

Introduction and Background

- Ultimately, Sandbox environment is artificial – can be detected
- Why bother?
- Wide range of detection techniques
  - Registry
  - Processes
  - Timings
  - Human interaction
  - Many more…
- What happens after detection?
  - End execution
  - Something else…

SOPHOS

Example Malware Families

Andromeda

- Sandbox detection:
  - Process names
  - Disk\Enum registry

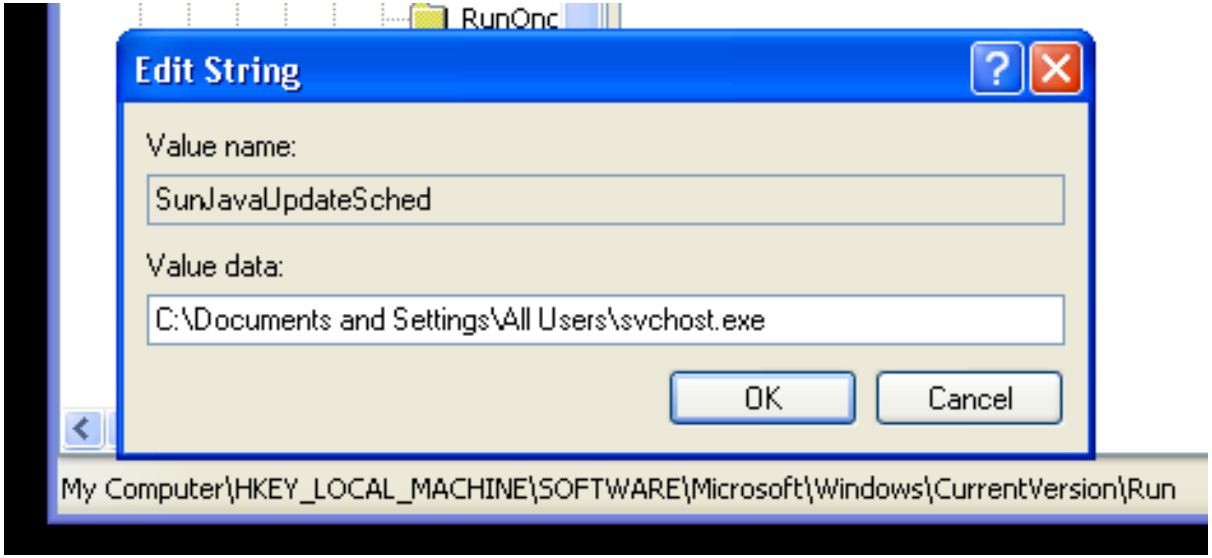
```
    cmp     dword ptr [ebp-364h], 'awmv'
    jz      short decrypt_bogus_payload
    cmp     dword ptr [ebp-364h], 'xobv'
    jz      short decrypt_bogus_payload
    cmp     dword ptr [ebp-364h], 'umeq'
    jz      short decrypt_bogus_payload

cause_exception_decrypt_genuine_payload: ; CODE XREF: sub_B1B98+B6↑j
                                         ; _1961:000B1DE7↑j ...
    mov     eax, [ebx+3Ch]
    lea     eax, [ebx+eax+18h]
    or      word ptr [eax+46h], 80h

decrypt_bogus_payload:  ; CODE XREF: sub_B1B98+102↑j
                        ; sub_B1B98+15C↑j ...
    push    ebx
    push    402544h
    call    sub_B1F03
```

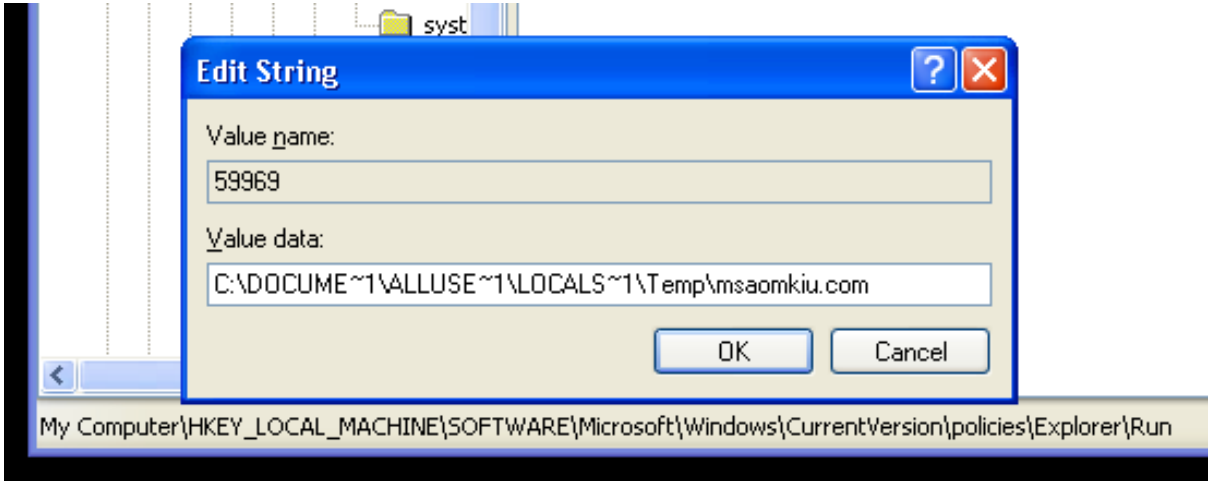
Andromeda – decoy behaviour

- EXE copied to static path name
- Runkey under CurrentVersion\Run
- Listens on TCP port



Andromeda – genuine behaviour

- EXE copied to randomised pathname
- Autostart registry entry under CurrentVersion\policies\Explorer\Run
- POST request to C2 server



Andromeda - Goals

- Hide C2 addresses
  - Blocked by fewer security products
  - Fewer abuse complaints, slower to take down
- Confuse analysis
  - Decoy behaviour believed to be genuine behaviour
- Lower the perceived threat level of the family
  - Appears relatively harmless

Andromeda - Consequences

- C2 addresses survive for longer
- Public embarrassment
- Downgrade threat severity of family
- **Not** failure to classify sample as malicious

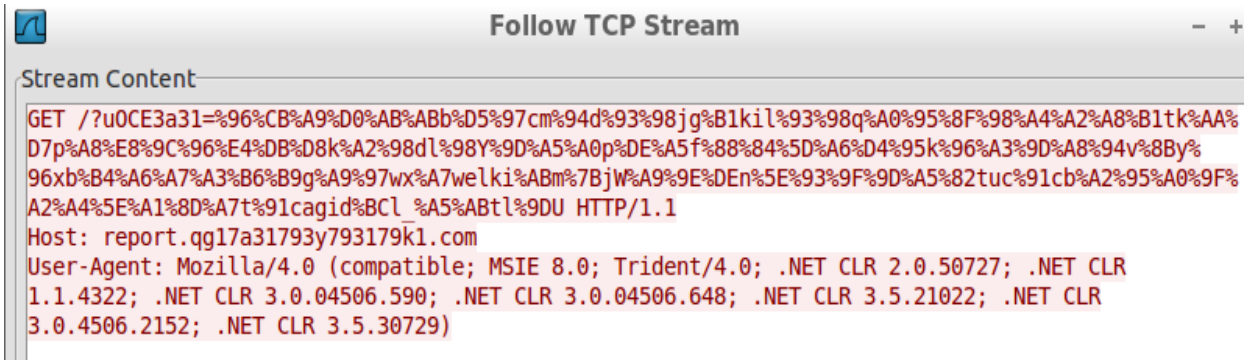
Simda

- Wide range of Sandbox detection techniques used
  - Evidence of analysis tools – registry, process names
  - ProductID of public sandboxes
  - Disk names + more

```
SYSTEM\CurrentControlSet\Services\IRIS5
Software\eEye Digital Security
SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Wireshark
SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\wireshark.exe
SOFTWARE\ZxSniffer
SOFTWARE\Cygwin
SOFTWARE\Cygwin
SOFTWARE\B Labs\Bopup Observer
AppEvents\Schemes\Apps\Bopup Observer
Software\B Labs\Bopup Observer
SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Win Sniffer_is1
Software\Win Sniffer
```

Simda - Behaviour

- Collect system information, send to C2
  - ProductID, computer name etc + Sandbox detection status



- If Sandbox detected, enter infinite loop
- Can also enter infinite loop depending on server response
  - IP address of Sandbox machine appears to be added to blacklist
  - Subsequent infections from real machines on same IP receive infinite loop response from server

Simda - Goals

- Hinder analysis
  - Further malicious components not dropped/downloaded
- Identify researcher IP addresses and hinder **future** analysis
- **Not** hide C2 addresses

Simda - Consequences

- True nature of the threat not appreciated
- Failure to detect secondary components
- Sandbox suffers in the same way for future samples, even if hardened against detection techniques, while same IP used

Vundo

- Very long-lived adware distributing family
- Multiple detection techniques
- E.g. check registry for VM strings in *SystemBiosVersion* value under HKLM\HARDWARE\DESCRIPTION\System

Vundo - Behaviour

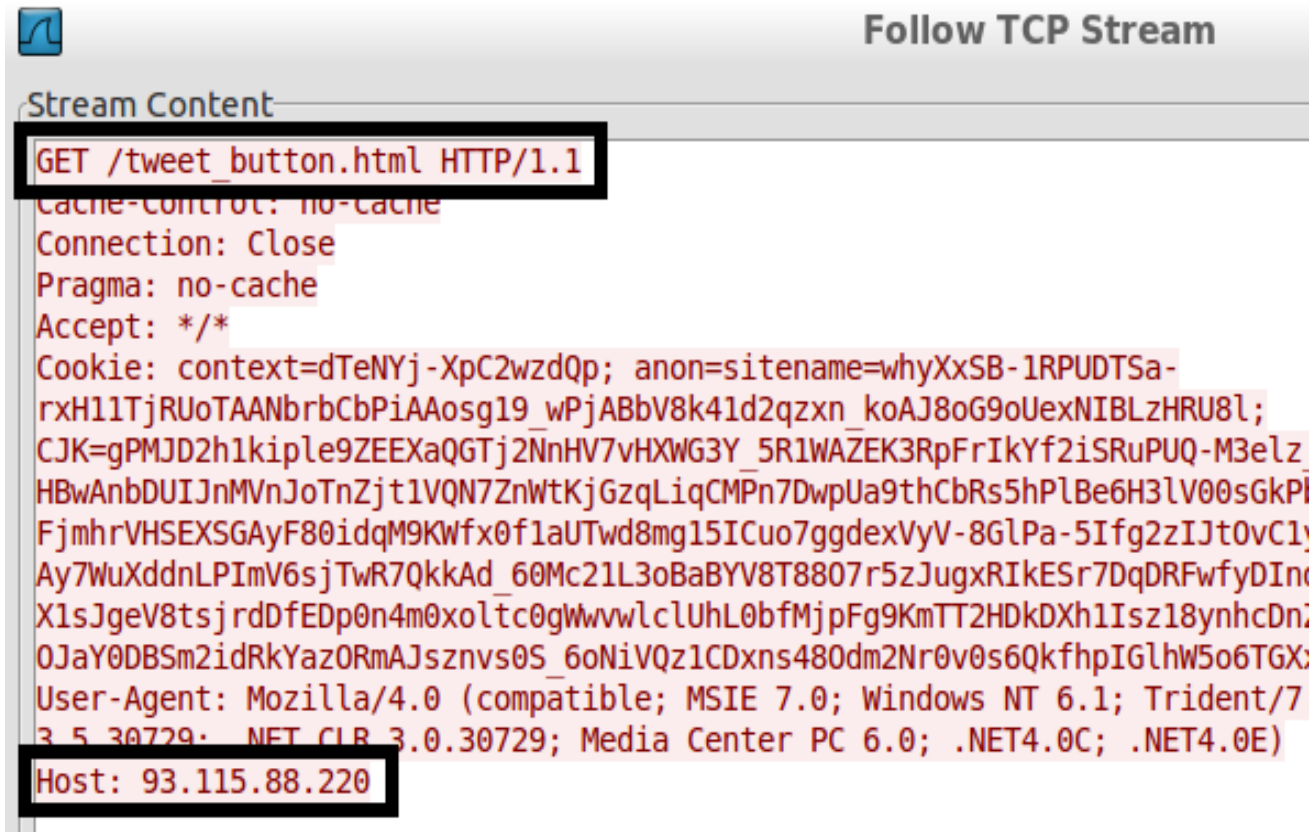
- Decoy HTTP request when Sandbox detected

- Decoy:

http_requests
request: http://12.6.182.165/adj/Category.aspx

Vundo - Behaviour

- Genuine HTTP request:



Vundo - Goals

- Conceal genuine C2 address
- Misdirect attention to decoy address
- Induce false positive

Vundo - Consequences

- Genuine C2 address survives for longer
- Resources misdirected to decoy address
- Potential FP

Shylock

- Banking family, downloads dynamic configuration file at runtime
- Multiple Sandbox detection techniques – process names, registry clues etc
- Strategy, post-detection has changed over time
  - Older variants would end execution
  - Newer variants appear to carry on as normal…

Shylock - Behaviour

- Sends large amount of machine information to C2 during execution
- Includes installed software, OS version + more

Shylock - Behaviour

- Includes name of AV installed and flag if VM detected: *VirtualMachine=Yes*

```
||||AntiMalwares=Sophos; VirtualBox|||||VirtualMachine=Yes|||||
```

Shylock - Behaviour

- Different configuration data delivered by server depending on VirtualMachine flag
- If VM detected, basic config delivered:

```
<hijackcfg>
        <botnet name="net2"/>
        <timer_cfg success="1800" fail="1800"/>
        <timer_log success="1200" fail="1200"/>
        <timer_ping success="1800" fail="1800"/>
        <urls_server>
                <url_server url="https://bai.su/index.php"/>

                <url_server url="https://sxo.su/index.php"/>

                <url_server url="https://pfh.cc/index.php"/>
        </urls_server>
                <httpinject value="on" url="/files/hidden7710777.jpg"


</hijackcfg>
```

Shylock - Behaviour

- No VM detected, more advanced config delivered
- Different URL paths, extra modules, different web inject file

```
        <archiver url="https://lud.su/files/rar.exe" cmd="a -r -dh -ep2 -v500k"/>

        <url_update md5="9fd741c8251fce276dfa587af274e045" url="/files/010-update-

        <httpinject value="on" url="/files/010-update-d9hbjz6/hidden7770777.jpg" m
        <grabemails value="off"/>
<plugins>
        <plugin name="BackSocks" url="/files/010-update-d9hbjz6/bsds.gsm" value="1
        <plugin name="DiskSpread" url="/files/010-update-d9hbjz6/dsp.psd" value="o
        <plugin name="MessengerSpread" url="/files/010-update-d9hbjz6/msg.gsm" val
        <plugin name="PGP" url="/files/010-update-d9hbjz6/pgp.asc" value="on" cmd=
</plugins>
```

Shylock - Goals

- Conceal existence of secondary modules
- Hide nature of advanced functionality – web injects
- Hide further network infrastructure – additional C2 addresses

Shylock - Consequences

- Failure to detect further modules
- Unaware of extra C2 addresses
- Advanced functionality not appreciated – no mitigations

SOPHOS

Categorisation of Techniques and goals

Techniques and Goals

Technique	Description	Example	Goal
Alternative, benign behaviour	The true nature of the sample is hidden along with data such as C2 addresses, to be replaced with different, more benign behaviour	Andromeda decoy pathname and listening socket	Conceal C2 addresses, extend life-time of network infrastructure, Reduce level of community knowledge about threat

Techniques and Goals

Technique	Description	Example	Goal
Blacklisting	Artifacts such as IP address are identified as potentially belonging to researchers, normal execution will not take place from these addresses even if other checks pass	Simda reports detected Sandboxes to C2 server, subsequent requests from real machines from same IP are instructed to enter infinite loop by server	Prevent researchers from further understanding the threat, build up list of likely security company IP addresses

Techniques and Goals

Technique	Description	Example	Goal
Decoy addresses	Alternative C2 addresses are substituted for the genuine value when artificial environment is detected	Vundo beacons to decoy address when first executed	Conceal genuine C2 address, divert attention to fake address, potentially induce false positives

Techniques and Goals

Technique	Description	Example	Goal
Fake configuration data	Configuration information returned by C2 servers is adjusted based on whether a Sandbox was detected	Shylock serves up dummy config file and dummy web injects if a Sandbox was detected	Conceal extra functionality not evident from the sample through server interaction, hide targeted URLs and injected code, hide existence of further modules

SOPHOS

Consequences of Failure

Consequences of Failure

- C2 address lasts longer
- Advanced features remain hidden
- Network interaction can no longer be analysed
- Misallocation of resources
- False positive
- Public embarrassment

SOPHOS

Protection

Protection

- Analysis environment must appear as much like a real environment as possible
  - VM hardening
  - Custom hypervisor
- Use physical machine
  - Management difficulties
  - Scalability
- Detect Sandbox detection techniques
  - Understand and detect every possible technique
  - Arms race
- Execute in different environments, isolate differences
  - Use un-hardened goat machine
  - Twice as many resources

SOPHOS

Conclusion

Conclusion

- Sandboxes becoming more widespread
- Broad range of data extracted
- Despite increased legitimate use of virtualisation, many malware families treat VM with suspicion
- Be wary of output from Sandbox
- Difficult to detect that we are being fed false information

SOPHOS