Fobos Malvertising Campaign Delivers Bunitu Proxy Trojan via RIG EK

malwarebreakdown.com/2018/03/21/fobos-malvertising-campaign-delivers-bunitu-proxy-trojan-via-rig-ek/

March 22, 2018

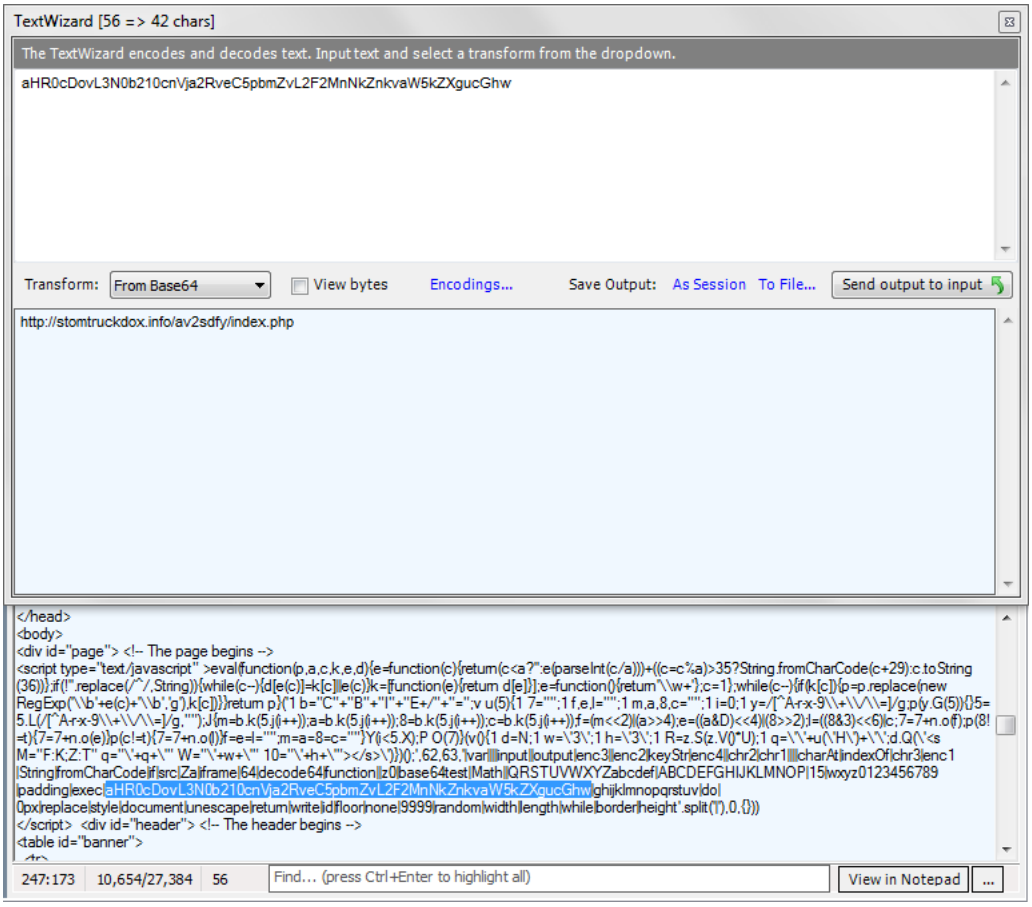
Originally posted at malwarebreakdown.com
Follow me on Twitter

Traffic from 03/21/18:

Destination IP	Dst Port	Host/Domain/Subdomain	Info
			GET / HTTP/1.1
88.198.94.53	80	stomtruckdox.info	GET /av2sdfy/index.php HTTP/1.1
92.53.107.18	80	92.53.107.18	POST /?NDk5OTA2&iOOZnMBdLpcrw&XNZbRzXCQZNY=dW5rbm93bg…
92.53.107.18	80	92.53.107.18	GET /?NTM3MTE3&kygcJtdEd&EZUAsHPSlmaVKU=Y2FwaXRhbA==&…
92.53.107.18	80	92.53.107.18	GET /?NTUzNzgy&ybdJRN&GvwwprdlENxM=cmVwb3J0&RevwwSpJz…

The first part of the redirection chain shown above would be from the Fobos decoy site.

The decoy site contains the following Base64 encoded string:



The decoded string on the decoy site points to the next step in the redirection chain, the pre-landing page:

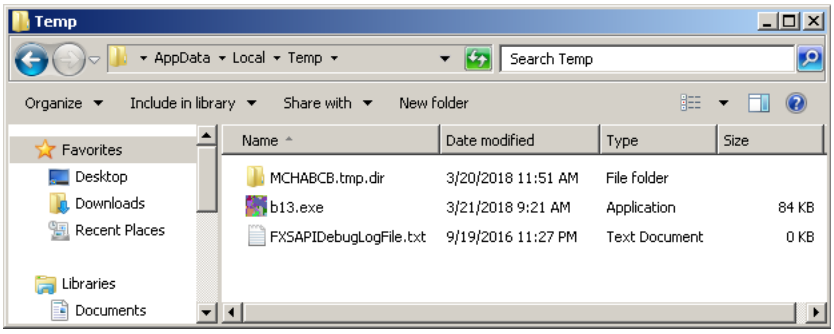
Unpacked and beautified: https://pastebin.com/dy646La6

After the pre-landing page comes the POST request to the RIG EK landing page at 92.53.107.18. Finally, after successfully exploiting my system, the Fobos campaign used RIG EK to deliver the Bunitu proxy Trojan. Below are some details about the infection.

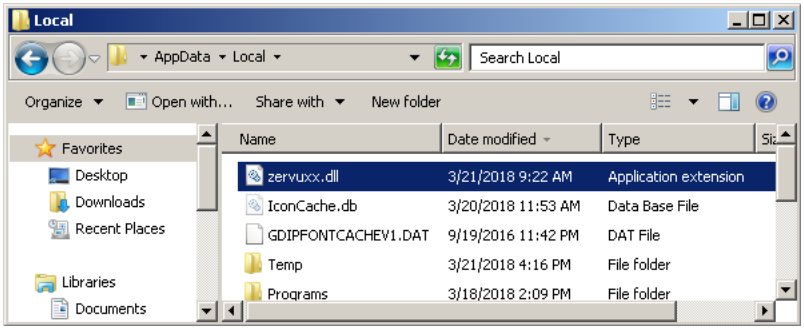
Analysis

File System

Payload downloaded to %Temp%:



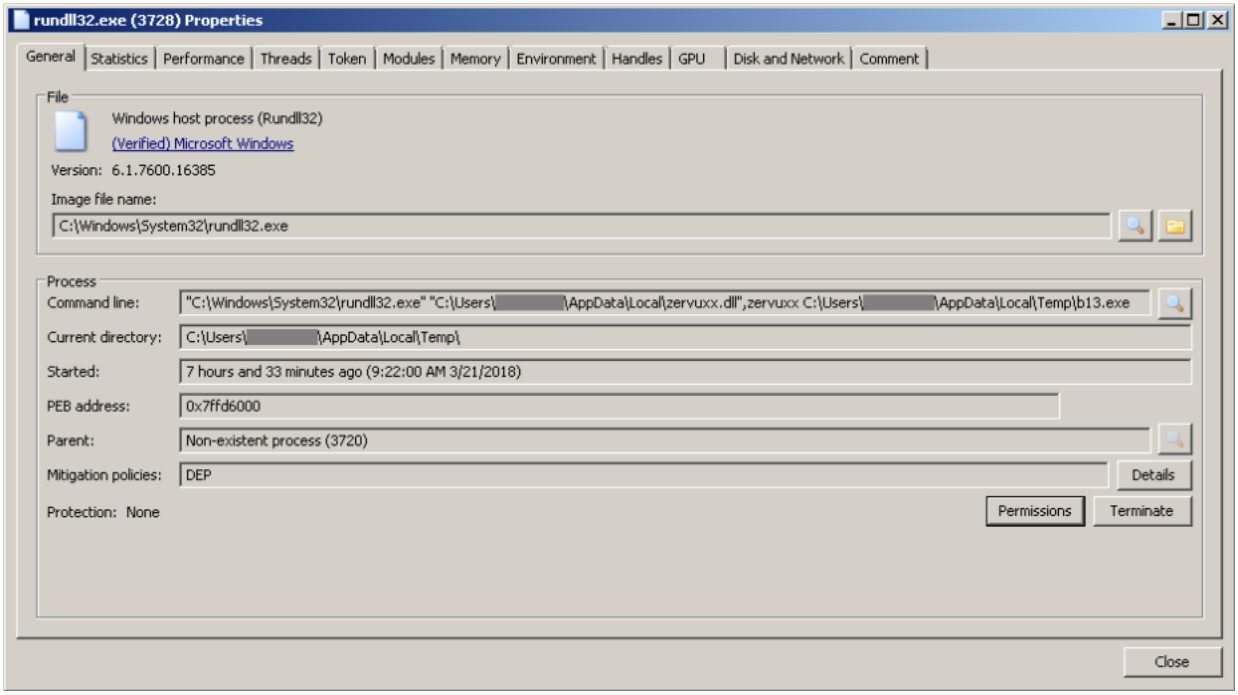
Process b13.exe (PID: 2616) created file zervuxx.dll in %LocalAppData%:



Processes Created

- Command line:
  “C:WindowsSystem32netsh.exe” advfirewall firewall add rule name=”Rundll32″ dir=out action=allow protocol=any program=”C:Windowssystem32rundll32.exe”
  Parent PID: 2616
  Child PID: 576
- Command line:
  “C:WindowsSystem32netsh.exe” advfirewall firewall add rule name=”Rundll32″ dir=in action=allow protocol=any program=”C:Windowssystem32rundll32.exe”
  Parent PID: 2616
  Child PID: 876

- Command line:
  “C:WindowsSystem32rundll32.exe” “C:Users[User]AppDataLocalzervuxx.dll”,zervuxx C:Users[User]AppDataLocalTempb13.exe
  Parent PID: 2616
  Child PID: 3728



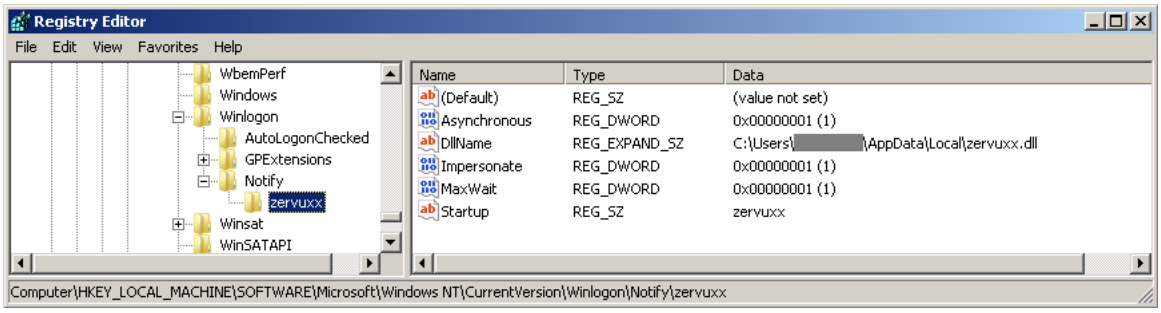
Registry

Keys created:

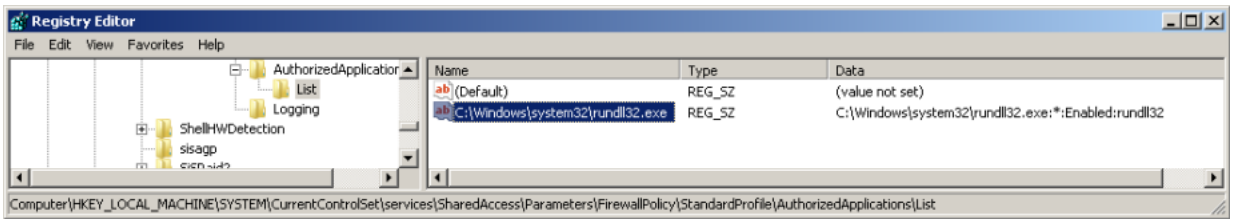
- HKLMSOFTWAREMicrosoftWindows NTCurrentVersionWinlogonNotify
- HKLMSOFTWAREMicrosoftWindows NTCurrentVersionWinlogonNotifyzervuxx
- HKLMSystemCurrentControlSetservicesSharedAccessParametersFirewallPolicyStandardProfileAuthorizedApplicationsList

Values set:

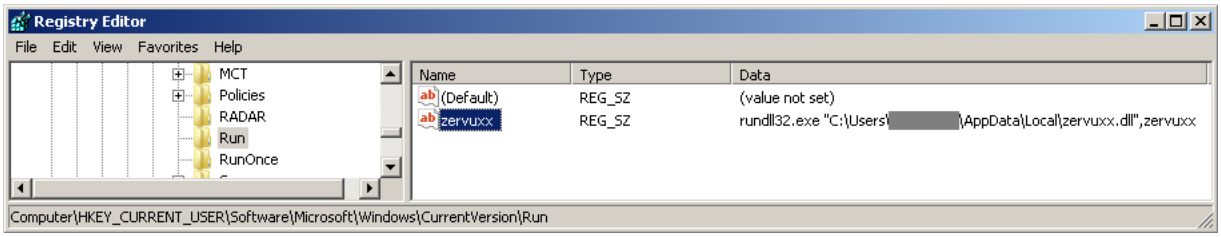
- HKLMSOFTWAREMicrosoftWindows NTCurrentVersionWinlogonNotifyzervuxxImpersonate
- HKLMSOFTWAREMicrosoftWindows NTCurrentVersionWinlogonNotifyzervuxxAsynchronous
- HKLMSOFTWAREMicrosoftWindows NTCurrentVersionWinlogonNotifyzervuxxMaxWait
- HKLMSOFTWAREMicrosoftWindows NTCurrentVersionWinlogonNotifyzervuxxDllName
- HKLMSOFTWAREMicrosoftWindows NTCurrentVersionWinlogonNotifyzervuxxStartup



HKLMSystemCurrentControlSetservicesSharedAccessParametersFirewallPolicyStandardProfileAuthorizedApplicationsListC:Windowssystem

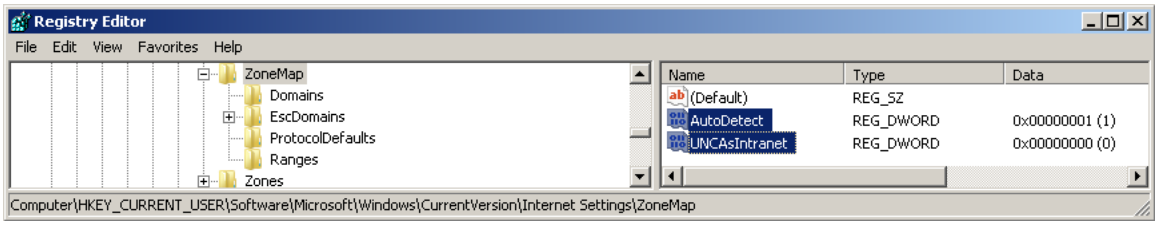


HKCUSoftwareMicrosoftWindowsCurrentVersionRunzervuxx



Set by b13.exe (PID: 2616)

- HKCUSoftwareMicrosoftWindowsCurrentVersionInternet SettingsZoneMapUNCAsIntranet
- HKCUSoftwareMicrosoftWindowsCurrentVersionInternet SettingsZoneMapAutoDetect



Mutex

Mutex created:

Sessions1BaseNamedObjectsdrofyunfdou

DNS

Queries and responses:

c.cawexdom.net -> 124.56.221.48
e.cawexdom.net -> 71.19.200.66

HTTP Traffic – Pre-Infection

- 88.198.94.53 – stomtruckdox.info GET /av2sdfy/index.php – Fobos
- 92.53.107.18 – POST and GET – RIG EK

Hashes and Reports

SHA256: ab0987156a279050e632aa5810d2d2355bf65c611d8b563bd73ef3392948bb3a
File name: Pre-Landing Page.txt

SHA256: a36204a8c830f420475a7e8b3dde7f29d80e6dffb15facf77f6b4fe8f78d7ce6
File name: RigEK Landing Page.txt

SHA256: 971c424d839bed4037a62f85791beb559f43e77d67a83590274478bdcf0c4563
File name: RigEK Flash Exploit.swf

SHA256: 8e8ac821d17dbbbecf0afabf93b1f8fd35a333215f363acbaa826851f7ad4286
File name: b13.exe
Hybrid-Analysis

SHA256: e7ac8ae86345db9a6087d4c3e99b8f8cd52ee0bf1ad626866af5452434c87322
File name: zervuxx.dll
Hybrid-Analysis

Samples

Samples.zip

Password is “infected”

Published by malwarebreakdown

Just a normal person who spends their free time infecting systems with malware. View all posts by malwarebreakdown