TA-505 Cybercrime on System Integrator Companies

marcoramilli.com/2019/11/12/ta-505-cybercrime-on-system-integrator-companies

View all posts by marcoramilli November 12, 2019

Introduction

During a normal monitoring activity, one of the detection tools hits a suspicious email coming from the `validtree.com` domain. The domain was protected by a Panama company to hide its real registrant and this condition rang a warning bell on the suspected email so that it required a manual analysis in order to investigate its attachment.
Digging into this malicious artifact opened up to a possible raising interest of the infamous **TA505** in **System Integrator Companies** (companies in which have been found that threat).

Technical Analysis

During the past few weeks suspicious emails coming from the `validtree.com` domain was detected: they were addressing System Integration Companies. The domain validtree.com is registered through namecheap.com on 2017-12-07T15:55:27Z but recently renewed on 2019-10-16T05:35:18Z. The registrant is protected by a Panama company named WhoisGuard which hides the original registrant name. Currently the domain points to 95.211.151.230 which is an IP address assigned to LeaseWeb a VPS hosting provider located in Netherland, Europe. Attached to the email a suspicious word document was waiting to be opened from the victim.

Hash	7ebd1d6-fa8c21b0d0c015475ab8c7225f949c13a33d0a39b8c069072a4281392
Threat	Macro Dropper
Brief Description	Document Dropper
Ssdeep	384:nFZ5ZtDGGkLmTUrioRPATRn633Dmej0SnJzbmiVywP0jKk:n1o-qwT2J633DVgiVy25

By opening the word document the victim displays the following text (Image1). The document tempts the victim in enabling the macro functionality in order to re-encode the document with readable charsets by translating the current encoding charset to the local readable one.

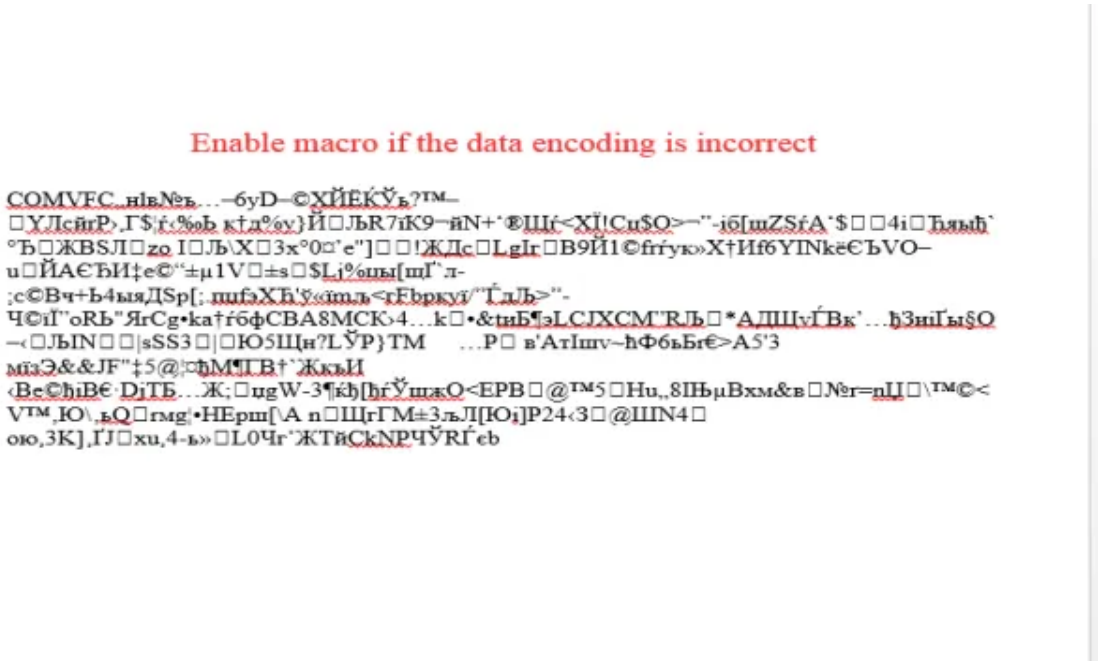

Image1: Word Document Content

A transparent Microsoft-word-shape placed on top of the encoded text avoids the victim to interact with the unreadable text. That document holds two VBA-Macro functions which were identified as a romantic `AutoOpen` and an additional one named `HeadrFooterProperty`. Interesting to note that the document had no evidences on VT (during the analysis time), so it could be a revamped threat or a totally new one! The two Macros decoded a Javascript payload acting as a drop and execute by using a well-known strategy as described in: “Frequent VBA Macros used in Office Malware”. The following image shows the decoding process. A first round of obfuscation technique was adopted by the attacker in order to make harder the analyst’s decoding process. That stage implements an obfuscated Javascript embedded code which decodes, by using a `XOR` with `key=11`, a third Javascript stage acting as drop and execute on `66.133.129.5` resource. That IP is assigned to Frontier Communications Solutions: a NY based company.

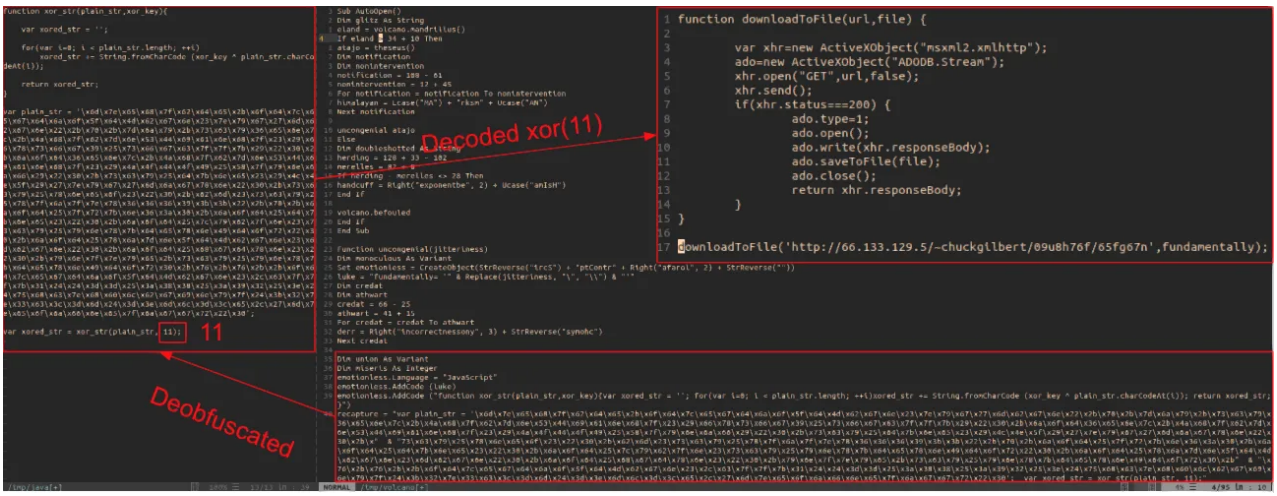

Image2: Deobfuscation Steps from obfuscated VBA to Clear “evaled” javascript

It was nice to read the obfuscated code since the variable names where actually **thematically** chosen per function. For example the *theseus* function is obfuscated with “divine terms”, one of my favorite was actually the following conditional branch: `If pastorale / quetzalcoatl <`

`57 Then ...` , which actually was always true ! (`quetzalcoatl` is “feathered serpent” a `aztech` god, while pastorale is an evocative composition often used for cite or pray to gods).
Another fun fact was in the variable name the attacker attributed to the string “JavaScript”: *emotionless*. In particular the attacker refers to JavaScript through the object “ `emotionless.Language` ”. Funny isn’t it ?
The final javascript downloader aims to drop a file from `http://66[.133[.129[.5/~chuckgilbert/09u8h76f/65fg67n` placing it into the system temporary directory and naming it `nanagrams.exe` . Finally it runs that windows PE file on the victim machine.
During the analysis-time the dropping URL was not working, indeed the dropping URL contains a `surprise.php` . Actually, a misconfiguration of the dropping website allowed us to visualize its source code. As shown in the following image (Image3) the page tracks the visitors through an iframe pointing to: `http[://tehnofaq[.work` and through a random loop redirects the downloader script to a different dropping URL.

Image3: Redirecting script

Building a re-directors or proxy chains is quite useful for attackers in order to evade Intrusion Prevention Systems and/or protections infrastructures based upon IPs or DNS blocks. In such a case the redirection script pushes to one of the following domains by introducing the HTML meta “refresh” tag, pointing the browser URL to a random choice between 4 different entries belonging to the following two domains:

- `http[://com-kl96.net`
- `http[://com-mk84.net`

Possible Link with TA-505

The used infrastructure, by analyzing the dropping urls, looks like an old infrastructure used for propagating Ransomware. Indeed it’s possible to observe many analogies with the following dropping urls belonging to a previously utilized Ransomware threat:

- `http[://66.133.129.5/~kvas/`
- `http[://66.133.129.5/~nsmarc1166/`
- `http[://frontiernet.net/~jherbaugh/`

The infrastructure used in the attacks suggests the involvement of the cybercrime group **TA505**. The TA505 group, that is known to have operated both the**Dridex** and **Locky**malware families, continues to make small changes to its operations. **TA505** hacking group has been active since 2014 focusing on Retail and banking sectors.
Recently security experts at Proofpoint observed the notorious TA505 cybercrime group that has been using a new RAT dubbed SDBbot, it is a backdoor that is delivered via a new downloader

dubbed Get2 that was written in C++. The dropper was also used to distribute other payloads, including FlawedGrace, FlawedAmmyy, and Snatch. The used URLs in the attack have the same pattern associated with the notorious crime gang, the researchers also pointed out that the IP addresses (i.e. 66.133.129.5) observed in the attacks were involved in previous campaigns delivering Locky and Dridex malware.

Unfortunately, I was not able to analyse the final payload of the attack chain that was still not available at the time of the analysis. **The final stage malware analysis is essential to attempt to attribute the attack to a specific threat actor**. The evidence and artifacts collected in this analysis suggest two possible scenarios:

- TA505 group is expanding his operations, but it still controlling an infrastructure involved in previous attacks across the years. The threat actors still leverage this infrastructure for "hit and run" operations or to test new attacks technique and tools avoiding to expose their actual infrastructure. Both options are interesting, **but only the knowledge of the final stage malware could give us a wider view on the current operations of the group**.
- Another threat actor, likely financially motivated, is leveraging the same infrastructure used by TA505 and used it to make it harder the analysis and the attribution of the attacks.

Conclusion

An interesting Maldoc acting as drop-and-execute was identified and spotted in the wild targeting System Integrator based in Europe . From the described analysis we attempted to identify the attacker by observing he was exploiting an old infrastructure behind `66.133.129.5` as a dropping websites.
During the analysis time the attack-path was still incomplete and the attacker didn't weaponize the dropping websites yet, but the spread document is able to grab content from specific URLs and to run directly on the victim machine.
The used strings for obfuscating the dropper were actually fun and "thematic". For example strings like "madrillus", "vulcano", "pastorale", "quetzalcoatl" remind an ancient culture (mandrillus, vulcano and quetzalcoatl) while objects like "emotionless" assigned to a specific programming language reminds a witty attacker.

Since no final stage was obtained so far, **attribution is quite hard,** but TTPs suggest a TA-505 attacker, due to the collected artifacts and to the analyzed URLs.

Indicator of Compromise (IoC)

Hash: 7ebd1d6fa8c21b0d0c015475ab8c7225f949c13a33d0a39b8c069072a4281392
URL:
http://66[.133[.129[.5/~chuckgilbert/09u8h76f/65fg67n
http[://tehnofaq[.work
http[://com-kl96.net/new.php?a=269321&c=wl_con&s=702w'
http[://com-mk84.net/new.php?a=269321&c=wl_con&s=702w'
http[://com-kl96.net/new.php?a=269321&c=job&s=702j'
http[://com-mk84.net/new.php?a=269321&c=job&s=702j'

Yara Rules

```
rule TA505_Target_SystemIntegrators_sample {
   meta:
      description = "TA505 target System Integrators"
      date = "2019-11-11"
      hash1 = "7ebd1d6fa8c21b0d0c015475ab8c7225f949c13a33d0a39b8c069072a4281392"
   strings:
      $x1 = "*\\G{00020430-0000-0000-C000-
000000000046}#2.0#0#C:\\Windows\\system32\\stdole2.tlb#OLE Automation" fullword wide
      $s2 = "*\\G{2DF8D04C-5BFA-101B-BDE5-00AA0044DE52}#2.3#0#C:\\Program Files\\Common
Files\\Microsoft Shared\\OFFICE11\\MSO.DLL#Microsoft " wide
      $s3 = "'%TEMP%\\conjunctiva.exe'" fullword ascii
      $s4 = "rams.exe" fullword ascii
      $s5 = "*\\G{000204EF-0000-0000-C000-
000000000046}#4.0#9#C:\\PROGRA~1\\COMMON~1\\MICROS~1\\VBA\\VBA6\\VBE6.DLL#Visual Basic
For Applicat" wide
      $s6 = "WScript.Shell" fullword ascii
      $s7 = "\\nanagrams.exe" fullword ascii
      $s8 = "*\\G{00020905-0000-0000-C000-000000000046}#8.3#0#C:\\Program
Files\\Microsoftvolcano" fullword wide
      $s9 = " Office\\OFFICE11\\MSWORD.OLB#Microsoft Word 11.0 Object Library" fullword
wide
      $s10 = "PROJECT.THISDOCUMENT.AUTOOPEN" fullword wide
      $s11 =
"5\\x64\\x7b\\x6e\\x65\\x23\\x29\\x4c\\x4e\\x5f\\x29\\x27\\x7e\\x79\\x67\\x27\\x6d\\x6a\\x
 fullword ascii
      $s12 = "Project.ThisDocument.AutoOpen" fullword wide
      $s13 = "mistyeyed" fullword ascii
      $s14 = "(xor_key ^ plain_str.charCodeAt(i)); return xored_str;}" fullword ascii
      $s15 = "IVa.ExE'); StaRT " fullword ascii
      $s16 =
"65\\x2b\\x73\\x63\\x79\\x25\\x79\\x6e\\x78\\x7b\\x64\\x65\\x78\\x6e\\x49\\x64\\x6f\\x72\\
 fullword ascii
      $s17 = "costaTEMP%instantaneous" fullword ascii
      $s18 = "wdSeekCurrentPageHeader$$0" fullword ascii
      $s19 = "TEMP%in " fullword ascii
      $s20 = "conjecturalitygclamydospore" fullword ascii
   condition:
      uint16(0) == 0xcfd0 and filesize < 100KB and
      1 of ($x*) and 4 of them
}
```