NanoCoreRAT Behind an Increase in Tax-Themed Phishing E-mails

By Anthony Kasza

Published: 2016-02-09 · Archived: 2026-04-05 17:16:14 UTC

It seems every mainstream news event or holiday has an accompanying phishing campaign. Opportunistic actors hoping to capitalize on the public's attention are often seen sending phishing e-mails with themes related to the news or the season..

It happened this last holiday season and will likely continue to occur as long as email is around.

Unsurprisingly, as we near the U.S. deadline for filing our income taxes, Palo Alto Networks researchers have seen an increase in phishing emails specifically related to taxes. This blog details some recent trends we have been able to identify. Palo Alto Networks noticed both executable attachments and Microsoft Word documents with macros designed to download and execute files.

Tax-Themed Phishing

Looking through recent email attachments determined to be malicious by WildFire, we noticed a trend in subject lines involving tax forms using the keywords ‘report’, ‘tax’, ‘secure’ and ‘pin’. Pivoting from subject lines to the hash values and filenames of attachments included in the emails allowed us to expand our initial sample set. Finally, using the AutoFocus API and a bit of Python we were able to collect data about the samples included in the tax-themed phishing and build a data frame for further analysis.

Within the final sample set, we were able to identify 70 unique malware samples distributed through 2,062 email sessions between September 2, 2015 and January 28, 2016. As expected, email sender addresses were often spoofed to provide a sense of legitimacy.

Some examples of email sender addresses:

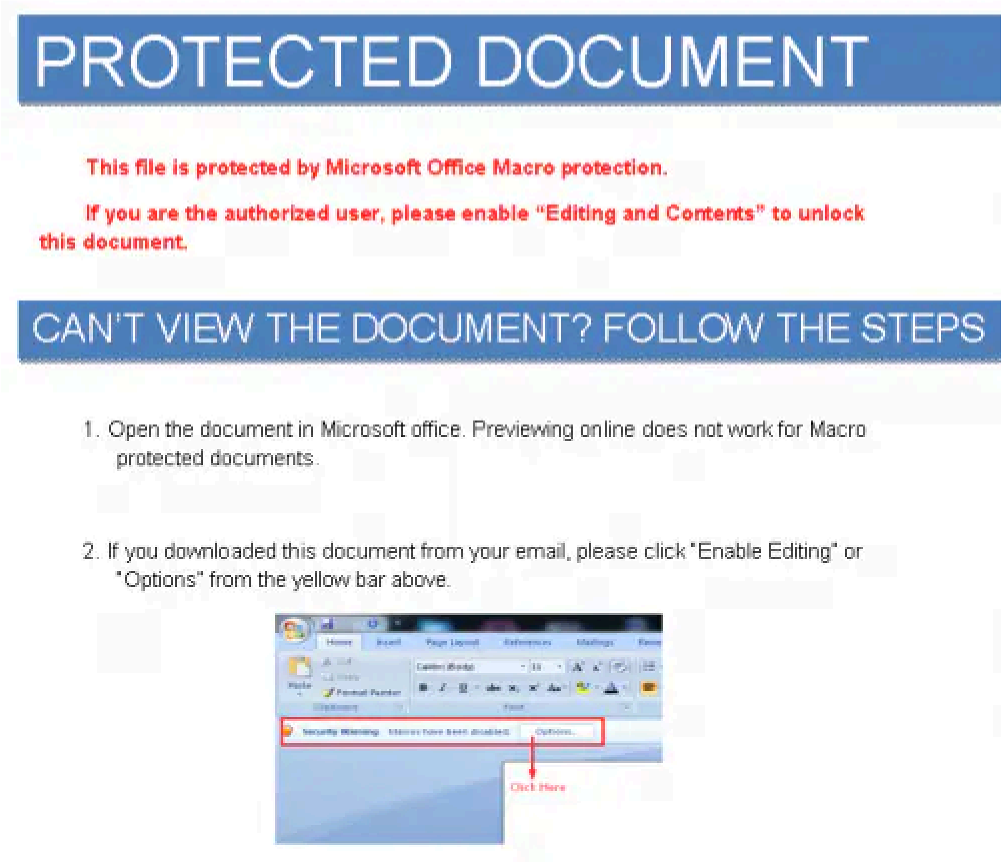
- 2015-autax-return@ato.gov.au
- 2015Refund@cra-arc.gc.ca
- 2015autaxreturn@ato.gov.au
- 2015tax-return@irs.gov
- 2015taxreturn-noreply@irs.gov
- 2015taxreturn@iras.gov.sg

We also noticed the source IP address of the emails primarily came from a free mail service called mail2world. The top 5 source IP addresses by session count were:

- 209.67.128.221 934 sessions
- 117.120.5.194 214 sessions

- 209.67.128.182 213 sessions
- 23.235.221.158 63 sessions
- 130.194.13.86 53 sessions

While some of the phishing email attachments were PE files, others were MS Word documents with malicious macros. One sample (119f3dd48e316f77974a7ec84c0fdecd943ceed77c30db9a6df0c1b0615b0ac0) included instructions on how to enable macros.

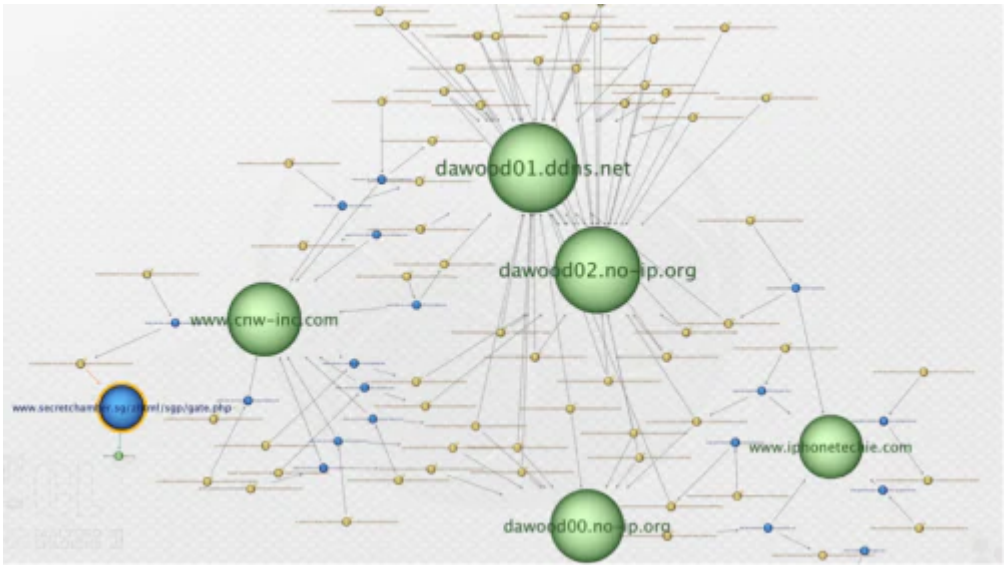


Using open source tools, the obfuscated file download functionality is easily located in the Word macro.

Looking at the malware contained in each email attachment, the payloads consisted predominantly of NanoCoreRAT or a generic macro downloader that would then download and execute NanoCoreRAT. The countries receiving these phishing messages align with what are believed to be country code indicators in malicious URLs and email attachment names.

Recipients of Tax-Based Phishing E-mails

Analyzing the malicious macro documents we observed for these tax-themed phishing attacks revealed that although there were a large number of unique samples, their behavior and infrastructure contained significant overlap.



In the above figure, we can easily see that six domains were in heavy use by most samples.

Second-stage download:

- www.cnw-inc[.]com

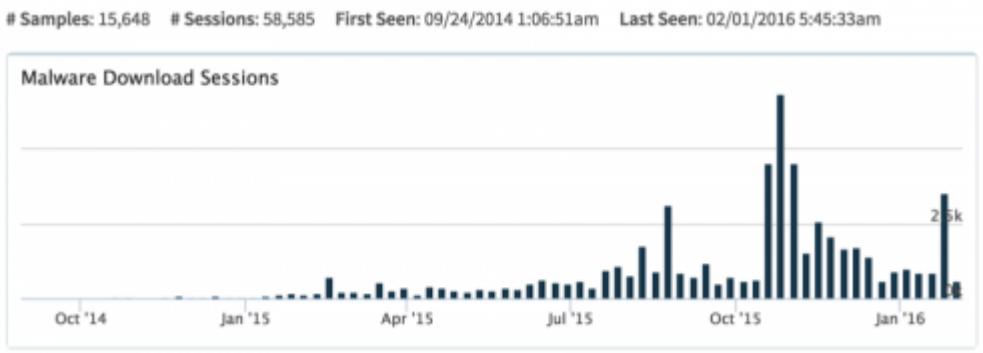
- www.iphonetechie[.]com

NanoCoreRAT Command and Control:

- dawood01.ddns[.]net
- dawood02.no-ip[.]org
- dawood00.no-ip[.]org

NanoCore

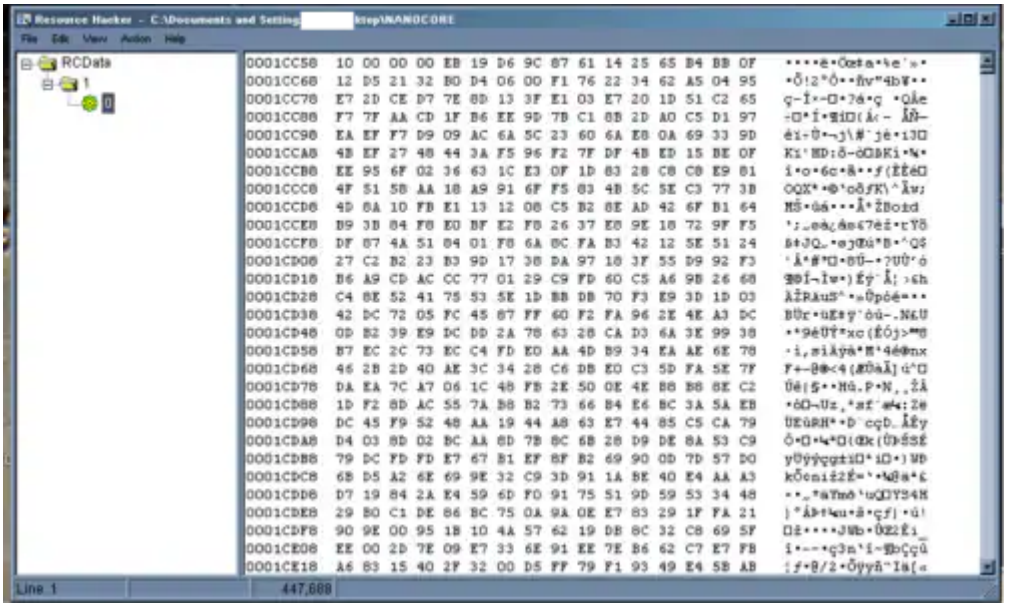
NanoCore is a commodity trojan developed in the .NET framework. According to Symantec, a fully cracked version of NanoCore 1.2.2.0 with premium plugins was released around March 2015 and has been seen targeting the energy sector. This release caused NanoCore to become increasingly popular with adversaries, especially the more frugal ones. Around April 2015 we observed a rise in activity involving NanoCore. We have observed its incorporation into tax-themed phishing since June 2015 and are continuing to see a general increase in activity since then. Below shows the upward trend Palo Alto Networks has seen in NanoCoreRAT being distributed since September 2014.



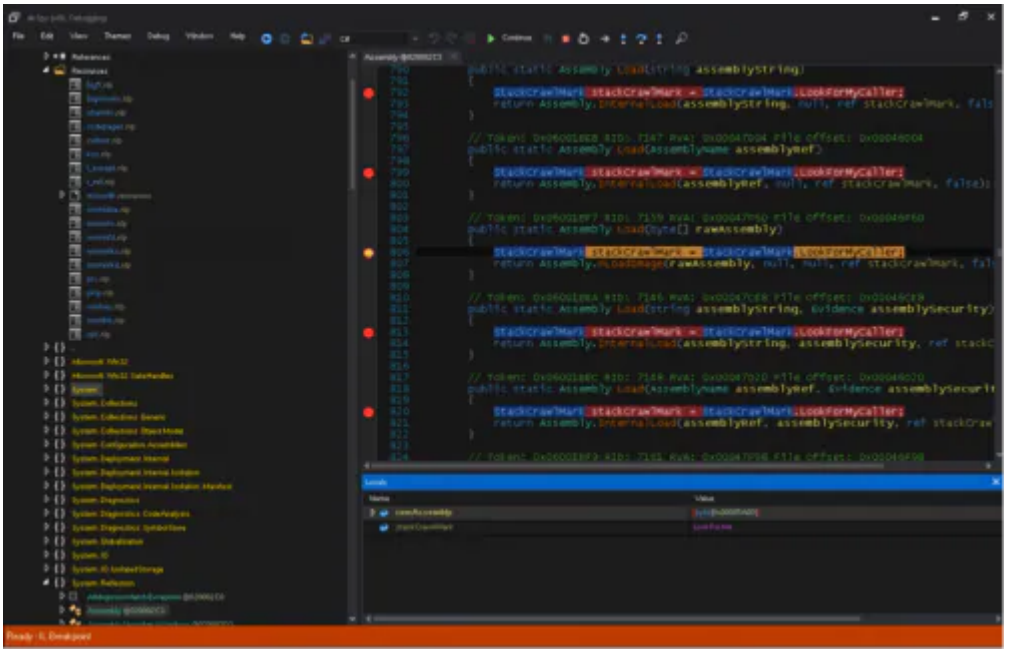
NanoCore is a modular RAT with many of its capabilities provided through plugins. Capabilities provided by the premium plugins we could identify include:

- keylogging and password "recovery"
- "stress testing" or DoS
- download, execute, or install other software
- remote CLI and UI
- registry editing
- socks proxy
- firewall modification
- webcam and audio controls

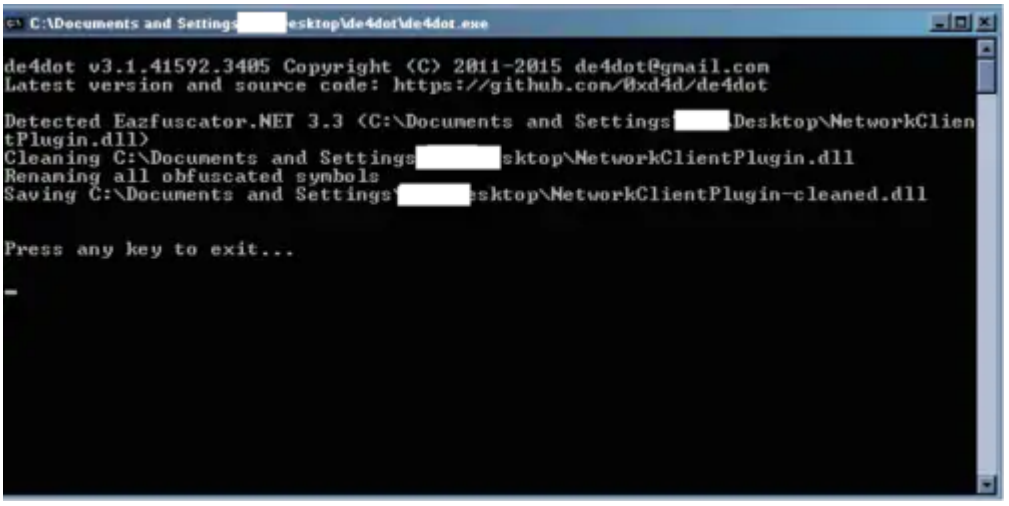
The plugins available to a NanoCoreRAT sample are encrypted and stored in the resource section of the PE file.



Using dnSpy as a debugger, we extracted the plugins included in sample 758f255abc102d53b7a4e8a8902da57076db9889cb80e81e8f1a344056f00c59 by setting breakpoints on all Assembly.Load calls, running the sample, and manually dumping the raw assembly bytes passed to those functions to disk as DLLs.



Most of the plugins included in this sample were obfuscated with Eazfuscater.NET 3.3 and easily deobfuscated using de4dot.



NanoCoreRAT uses a custom TCP protocol to connect to a server specified by the attacker on the port of their choosing. Below is the encrypted traffic sent by one sample to 54.152.254.8 on TCP port 4782:

```
00000000 40 00 00 00 52 5a 31 be 44 a9 01 f5 65 18 54 8e @...RZ1. D...e.T.
00000010 75 be e4 66 6a a4 0f e1 d0 4b 4e 6d 27 b6 19 a1 u..fj... .KNm'...
00000020 0b 21 07 b8 1a 57 60 42 0d 54 d8 4e 1b 04 54 6b .!...W`B .T.N..Tk
00000030 d5 8c 94 a0 76 88 6f 8a 05 88 dc ca 65 62 54 2b ....v.o. ....ebT+
00000040 fe d4 ab 7c
```

This sample uses DES to encrypt the traffic. It creates DESCryptoServiceProvider with a key from the Assembly Resource Guide Attribute and bytes from the resource section.

```
1  private static bool smethod_13()
2  {
3  byte[] array = Class8.smethod_16();
4  if (array != null)
5  {
6  ...
7  Guid guid_ = Class8.smethod_18(Assembly.GetExecutingAssembly());
8  Class8.byte_2 = Class8.smethod_19(byte_, guid_);
9  Class13.smethod_0(Class8.byte_2);
```

```
10  ...
11  }
12  private static Guid smethod_18(Assembly assembly_1)
13  {
14  Guid result = new Guid(((GuidAttribute)assembly_1.GetCustomAttributes(typeof(GuidAttribute), false)
    [0]).Value);
15
    return result;
16
    }
17
    private static byte[] smethod_19(byte[] byte_3, Guid guid_0)
18
    {
19
    Rfc2898DeriveBytes rfc2898DeriveBytes = new Rfc2898DeriveBytes(guid_0.ToByteArray(),
20  guid_0.ToByteArray(), 8);
21  return new RijndaelManaged
22  {
23  IV = rfc2898DeriveBytes.GetBytes(16),
24  Key = rfc2898DeriveBytes.GetBytes(16)
25  }.CreateDecryptor().TransformFinalBlock(byte_3, 0, byte_3.Length);
    }
```

```
48      public static void smethod_0(byte[] byte_0)
49      {
50          DESCryptoServiceProvider dESCryptoServiceProvider = new DESCryptoServiceProvider();
51          dESCryptoServiceProvider.BlockSize = 64;
52          dESCryptoServiceProvider.Key = byte_0;
53          dESCryptoServiceProvider.IV = byte_0;
54          Class13.icryptoTransform_0 = dESCryptoServiceProvider.CreateEncryptor();
55          Class13.icryptoTransform_1 = dESCryptoServiceProvider.CreateDecryptor();
56      }
57
58      // Token: 0x06000101 RID: 257 RVA: 0x00007144 File Offset: 0x00005344
59      public static byte[] smethod_1(object[] object_1)
60      {
61          Guid guid_;
62          return Class13.smethod_3(true, 0, 0, guid_, object_1);
63      }
64
65      // Token: 0x06000102 RID: 258 RVA: 0x0000715C File Offset: 0x0000535C
66      public static object[] smethod_2(byte[] byte_0)
67      {
68          return Class13.smethod_4(byte_0).object_0;
69      }
70
```

Locals

Name	Value
byte_0	{byte[0x00000008]}
[0]	0x72
[1]	0x20
[2]	0x18
[3]	0x78
[4]	0x8C
[5]	0x29
[6]	0x48
[7]	0x97
dESCryptoServiceProvider	{System.Security.Cryptography.DESCryptoServiceProvider}
BlockSize	0x00000040
BlockSizeValue	0x00000040
FeedbackSize	0x00000008
FeedbackSizeValue	0x00000008
IV	{byte[0x00000008]}
IVValue	{byte[0x00000008]}
Key	{byte[0x00000008]}
KeySize	0x00000040
KeySizeValue	0x00000040
KeyValue	{byte[0x00000008]}
LegalBlockSizes	{System.Security.Cryptography.KeySizes[0x00000001]}
LegalBlockSizesValue	{System.Security.Cryptography.KeySizes[0x00000001]}
LegalKeySizes	{System.Security.Cryptography.KeySizes[0x00000001]}
LegalKeySizesValue	{System.Security.Cryptography.KeySizes[0x00000001]}
Mode	CBC
ModeValue	CBC
Padding	PKCS7
PaddingValue	PKCS7
s_legalBlockSizes	{System.Security.Cryptography.KeySizes[0x00000001]}
s_legalKeySizes	{System.Security.Cryptography.KeySizes[0x00000001]}

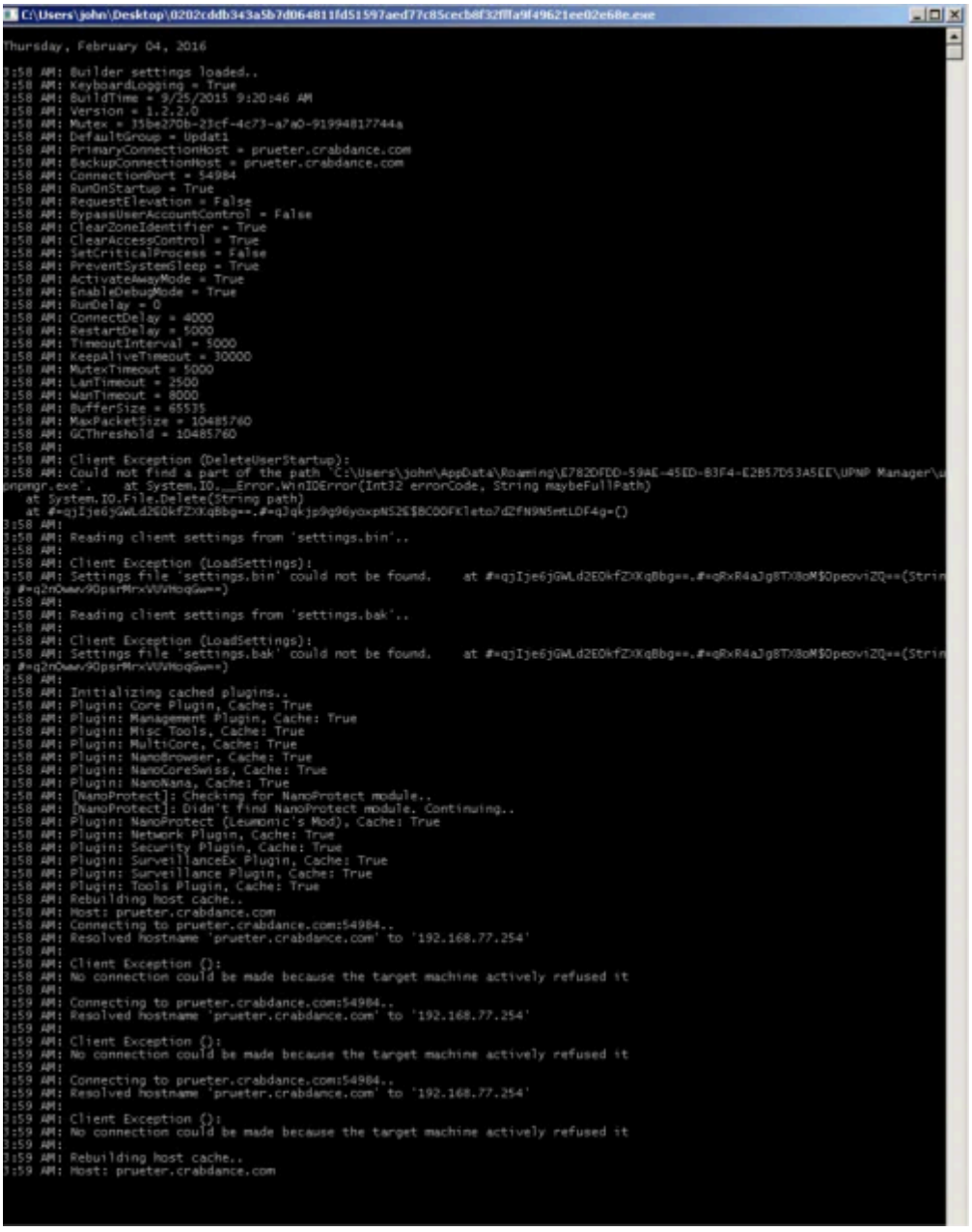
The DES key for this sample is 72 20 18 78 8C 29 48 97, we can use it to decrypt the traffic into the following:

00 00 00 00 12 DD DF 82 E7 AE 59 ED 45 B3 F4 E2 B5 7D 53 A5 EE 0C 14 57 49 4E 2D 48 55 46 44 39 33 41 52 36 32 32 5C 6A 6F 68 6E 0C 07 44 65 66 61 75 6C 74 0C 07 31 2E 32 2E 32 2E 30
.....Ýß,ç®YíE³ôâµ}S¥î..WIN-HUFD93AR622\john..Default..1.2.2.0
System Guid ComputerName\Username RAT Group Version

The bytes are stored in array2 and are encrypted with the following code and stored in the byte array named buffer.

```
byte[] buffer = Class13.icryptoTransform_0.TransformFinalBlock(array2, 0, array2.Length);
```

NanoCore can output messages to a console if the EnableDebugMode parameter is enabled in the RATs configuration.



Conclusion

Phishing is often how threat attackers gain access to targeted systems and user awareness is the first line of defense. Phishing isn't new but the increased distribution of the full-featured NanoCoreRAT implants is. Users should be made aware of the dangers that enabling macros poses. We have observed macro-based attacks on the rise in October of 2014

Palo Alto Networks customers with WildFire turned on would have been alerted to the presence of this threat on their networks. AutoFocus customers are able to further research both tax-themed phishing and NanoCoreRAT samples and trends.

Indicators

Email Subject Lines

[Attention] Your 2014 Tax Report

[Urgent Attention] Your 2015 Secure IP PIN

[ATO: URGENT] Your 2014 Tax Return Report!

[URGENT ATTENTION] Your 2014 Tax Return!

[ATO: ATTENTION] Your 2015 Tax Return PIN!

[IRS ATTENTION] Your 2015 Secure IP PIN!!!

[HMRC ATTENTION] Your 2015 Tax Report PIN!

[ATTENTION] Your 2015 Tax Return PIN!!!

Email Attachment Filenames

IRSReport.doc
CATAXREPORT.doc
2015TaxPIN.pdf.exe
[CRA]Report.pdf.exe
SGTAXREPORT.doc
[CRA]TaxReport.doc
[IRS]TaxReport.doc
[HMRC]TaxReport.doc
TaxReport!!.doc
SGTAXREPORT.pdf.exe
[CRA]ReadReport.doc
UKTaxReturnReport.pdf.exe
CATaxReturnReport.pdf.exe
[CA]Report.pdf.exe
[BE]TaxReport.pdf.exe
US2015TaxPIN.doc
AUTaxReport.pdf.exe
AU2015TaxPIN.doc
2015TaxPIN.doc
CRA-Report.doc.exe

TaxReport.doc
UKTAXREPORT.doc
AUTAXREPORT.doc
CATaxreturn.doc
[CRA]Report!.pdf.exe
FRTaxReport.pdf.exe

Email Attachment SHA256s

b633e5b9d6961f63dbf07ccd864903948a3c0772f2f66f86ad42c5b1faa0c539
a1bc606d12db420c511ba94f042021d34d84ba98a16c016445632ed03d37f909
bbbc92b4ebab54a3b7e35168a0e89ecbae701d3a04ea0df9bb5c132fcb8fa2aa
a89dd66865554cbe2b1ea6ff18653e964ac48ef585458d7f2d18f3083d039b39
6c1eb38781214b88cc9f9eb702ad9655f32e033ffa493e0954100b6be9c12d98
4b1b9fa256a6e6473c5ca25ce30ccdb4f955abb5e620d219dce85152d9e440ed
d910ffe4bb03c3b0066877b75c8ce5f5bc7ad1ae74908d96f7571bb75bf485f3
a827613e8a9d69f6401a25690e2282722b901b31f748c1ed2766e680bc14e77c
ba37d89a20a944cdee5cc4bd146cc225124091f9a576b1c5d6fa0239f3628b38
fc8da8715a9cab9643c63c7dacf83613478b11b2fc758d2b3b989ffbba9b93af
899e395fd22b8dc909a26c8fb380eac00e51e2b8766ef363d2a1c75335a40591
c4e0c88aa4c1a3da9a21114b22b546e238643146603ca667ea2158f142149507
b13305fe5d3c9e904ffe8d39fcc363f4fa799f5c57c854bf5a5e1ce9307942a4
200b1ed7f776d4ee32430ffdffefc76c44f359c19a7dff90e5b5ecdbef8e5608
3f1fc0757542fd80f216753d34ec27569f826d690a520d16017cd6f35acb4be8
fbcb8f3de748be39c396deea1f172213ff203f3997c575b017ed5e6e2c46ba18
119f3dd48e316f77974a7ec84c0fdecd943ceed77c30db9a6df0c1b0615b0ac0
71755fd086ccf44e384d59e91234906403aaf28d73fea96ffa052187c2824b6a
e2c3c2949f12556b5df7ead551eea2e9a0827dafdf385be2d1f470ba768be4f0
283152ea205f4098e221b6dab94e5c61619d507b4e8ad3613f7df4ffac35ba88
23067c7dd27eeeab574aa7cf65fd2b287c2ff794aed3589ff89419a71b740afd
ea97f1c48ed8e91e5e53683417893dc99f620acbd90b20b069e891c8875fa3ee
11b2db6fe850cbd373b5222e2512603e3bda0be749910e15d2961a373d56dde8
09a73ceeaf543a7741503c477af939aa59d13ba1d81983844a4b94bdfa27396a
6d3917640123e89a714cb0f165c91ae3ffcf8b7bb6321c57c96684952982fbef
4f60ebf97267480ab084e0851759b18111427e63628ba89a0deaea24c987cf3c
0175575982f1d298b980583cd48d3d7cdc14ce944352fd259a76f46a58bc609b
371fa8f45c0203d3470db7518571a8ced1070d2836e3d697e02c614d0b6fe401
a222d3095d93afbbc59f15ef9fce75dcfbd19eb9d619a8536fd8e49935220319
657758c09948c3203283fe61de51a31af77115e30b1f0e0b0296d40f97a2d615
d60d17f39de0d9298eb629d68276198793a16780260340fb8a2af35087a0ffa1
323cde2a163b8296159637c536c349756fccc2cf356fa084eb42dc5756627a4a
572b7dd0a742c5efda10b6ae40e764eb81db1add5736d14dd6dd9e091c711475
48912c24f24ea296ca00be255a9c8a27b8dd3c7b2755c0a562018e0f04ca5fc1

e18ba8f98204e754e66d3ab5b5bddef80d0a8e924cf29342ec746570d113d0ce
f10a42a4f135adf7e71b9f23454bf57d616cb5373135b7a70334f1a8921b12a2
fa4f12d6aa94d6196b68e304e31d7365c2ebeff465f87012c233d366f08abfed
326ba05909dc6244e00253ef610aea8904b935c617802d492d889363e3f27fa7
82c9b0b1076fb2709711142a62d04601896606bdb1647ae1a4e51d2158475138
6e21a9823b5b7ee7c6a2a7d2323afbd9693cd141cf9d1f80f2030b16a0df0937
5071acb947d01fc7298df97480a5701bfd1c15e629c7ddfe70c75fd8b3bc9b31
ca06f69759d2e331a1355af447daa857a5ca5bd8e7dd3d25d5c11f58c4a3cd0e
40ee213a2b2b26c5c48501e159dc30151d2a31056f4c9a32e256c397bf875b85
822445be43d5e383971ed3b9a63a9f4c17d0e8d067986cecd14e537f71a0e4f0
798e0e897035d4b821364435e6eaf620181b8096df65d73aea85ef84d7fd5c2c
80771e4e8155602b5e40aded581f1e141355942a5c8236ddbfcd9983ec8e4bfd
b5240a38cab5eea7610e902ac7e62b41c255d82eaaad7cfb39cd49029bf50804
8d6146bc12d170162ff2b542cf56b07aa91c970416b38ef274a95cd4ecb10063
6e15e471b76fea17cae4aea600a61680d53a8f857489bc818a7b88092bfdb724
96ffab6bc9b0d9f2d2e0388aea2c13a263e11c708bca309d5f3b1ffe77a5be5c
7c7434fc496f7cae0185e4ec40a17b41d24f8a2fdbeae9e64998426a1063e26b
d1778dd50c2a906bcc8e53372045dd3d976d5071ef8b3817ec28627fc0f4d8df
83f29a170ffcb9f13e630e1b240cfb0c75ff6854740ccf700e83af40a2dc770b
677ec33db3d3e9b20894bfc1280d3a9944413434cf4eae844d6f79d49bc372bd
6a8c5e6026e6a5d4561d4006ae7a3f0ab82d5ba4deb21c904684a6c3a5c75a7c
3118ca1232a55ee0d718c5efb2590d3af0a19d6a3861f4c7c56ecf0dcc3a8083
4eca6ea67d389ce85e41804bdb23acd7e34e585b3b92ce521636ffa35d877e32
fc83728faf8ca614e2798d64ed2eca2691354bf83ff5726d52badcd44787db14
87971bb9bdaea061ebea3d6903d6df359a13713e0d5aeda0a3fee0df852c3799
44b6807e0ea21d7f41ca09fa04a8bd1192fd568364a3ac5ba12a7c0de7d57a9d
455705d79026ddfc758cf069267b6975c677e2a28a0f553baca91a3f95d6dbbc
37160143a5064b505f050d8d37fbd2d2492c62afa599c9bbe0a6c5f0e20f3300
d175d0c65acebb61bdefd3e498bb24761c6ffd67c401060649d094e9a7d7753b
bf1e3483ec56fb480a88c6208f5ba2e51a69361b8cb26b8002f4c3bc562996fb
73935900282967ad8d1d0822f46c49cd69ae49e15bf63435db5074b6d932ba01
a34a3e1d0e427c9b112bd647fc5b53f1f8401e12bdcf16d6076dbc17fcaa7537
b11ac7fcb5d0427b922a8f6ba0bf6078647cb8bf3bed11ca43dc30f0f30157f2
6335b913b0a900e67155dab585249c1861912116bd53bb46055ee966511f97a8
cdc350df224011bd95f8fc04cfe355b44f1a3732ea7683339227baaa89a7935e
161a7c71330f0088b5bc06cc2a80fb1217e1a834d8ca87e749cdafa64f521bc5

Email Attachment Resolved Domains

agor0020.gotdns.ch
btint.net16.net
dawood00.no-ip.org
dawood01.ddns.net

dawood02.no-ip.org
www.cnw-inc.com
www.iphonetechie.com
www.pantech224.firstcom.com.sg
www.secretchamber.sg

NanoCore Deobfuscated Plugin SHA256s

ClientPlugin.dll	277f74d0ce633645c1a3a91b45f800f16385496d50c511084ccbd19c33a39b23
CoreClientPlugin.dll	8c18712257e04e0554a4fa8414906489bc4300ee71405719d43ce949decddf18
FileBrowserClient.dll	98b70d6b88b8fdf05d8da676fa7a48622c2d415cd5cf8e8a1f193dc6c65dc101
Lzma#.dll	ee05e8bd662e8e59c851b4053d2b34e8524cbe5356ee6c385b07d028a9dfb28d
ManagementClientPlugin.dll	3ad61e99f7a09c524121981f536b625fadcb27481d99ffe75938bb550be8883e
MyClientPlugin.dll	1e6cc9c0ee28a352611fd1a6b41f4a5e66019729b529d9177b14b25624533cad
MyClientPluginNew.dll	c986b9e146cb4f88dc68bea7927c76e0056e181b7b0de45fe4a221ce5e900d08
NanoCoreBase.dll	ea8ddf633460353ab0e641b97a370873b16ac4aef3e6ef6bffc2c4618256ab64
NanoCoreStressTester.dll	edd0e15cdf75f8158c5aae90db3e8c7d7705a247c5d807bc74c027c36ef6dc3d
NetworkClientPlugin.dll	6995887a9827808ca41ffbfddbeb93b8de9468387ec8958207a3eb9951d286f6
SecurityClientPlugin.dll	ee5cb353a3e4bdce3ac3b514e2e17e0dd0b04d787b4705c7cf1a681c0b422d85
SurveillanceClientPlugin.dll	beaf550d664abe4653fd0ddbdd1783894141b51272d8ac565556aa28e2ac847d
SurveillanceExClientPlugin.dll	5db139678bcfda1b46ddab1e2956b599da89a364230d16703a4ac0b02325a13a
ToolsClientPlugin.dll	a4f7a7dddbef1930d11609e4cd7604d1c3a75646db051499b1247b3b03b48692
MyClientPlugin.dll_2	7c1d77c3b41af227c5f6ae49000134420ce9fdd8d3050eceb5aa2358a31a4724

Additional Resources

- NanoCore and Unpacking the AutoIT Cryptor
- NanoCore: Another RAT tries to make it out of the gutter
